

AUDIRISK Web

Software de Auditoría Interna y de Sistemas Basada en Riesgos Críticos

Versión 7.5

Presentación del Software





Agenda

- **AudiRisk: Qué es y para Qué Sirve?.**
- Características del Software AudiRisk que agregan valor a las Organizaciones y las Auditorías.
- Especificaciones Técnicas del Software AudiRisk.
- Modalidades de Licenciamiento.
- Entregables que recibe el Usuario de AUDIRISK.
- Presentación detallada de los Módulos Componentes del Software AudiRisk.
- Beneficios de Utilizar AudiRisk.
- Usuarios del software AudiRisk.





El Software AUDIRISK

Ayuda a Modernizar enfoque y procedimientos de Aud Interna

Estado Actual de La Auditoría

1) **Enfoque Reactivo** – Detrás de los hechos conocidos ó riesgos ocurridos.
2) Sin herramientas de software de Auditoría Especializadas.
3) Auditoría a las operaciones, "Por Areas" (oficinas).
4) Auditoría "No basada en Riesgos" o sin considerar los riesgos críticos.
5) **No se evalúa control interno como base para diseñar Pruebas de Cumplimiento y Sustantivas.**
6) Cumplimiento limitado (parcial) de Normas de Auditoría (NAGAs, IIA, ISACA.

Estado Deseable - AUDIRISK

1) **Enfoque Proactivo** – Preventivo: Advierte a la Gerencia propensión a los riesgos antes que estos se presenten.
2) Uso de herramientas de software de Auditoría Especializadas.
3) Auditorías a las Operaciones "por procesos (del modelo de operación, procesos de TIC y servicios automatizados)".
4) Planeación y Desarrollo de la Auditoría "Basada en Riesgos Críticos".
5) **Evalúa diseño y efectividad de los Controles Existentes como base para diseñar las Pruebas de Cumplimiento y Sustantivas.**
6) Se planea y ejecuta de acuerdo con estándares de auditoría internacionales vigentes.





El Software AUDIRISK

Ayuda a Modernizar enfoque y procedimientos de Aud Interna

Estado Actual de La Auditoría  **Estado Deseable - AUDIRISK**

Estado Actual de La Auditoría

7) Auditoría sin utilizar el computador como herramienta - Alrededor del Computador

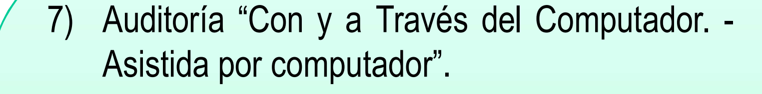
8) Poco Enfasis a los servicios de Sistemas de la Empresa (TICs).

9) Papeles de trabajo tradicionales – Hard Copy.

10) Seguimiento Manual a los hallazgos y recomendaciones de la Auditoría.

11) Débiles conocimientos en Gestión de Riesgos y Diseño de controles

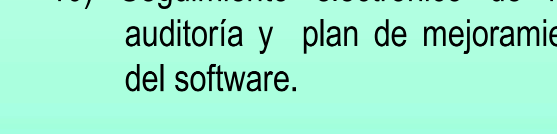
Estado Deseable - AUDIRISK



7) Auditoría “Con y a Través del Computador. - Asistida por computador”.

8) **Enfasis en los Servicios Automatizados. Los controles automatizados son el corazón del control interno**

9) Papeles de trabajo Electrónicos.



10) Seguimiento electrónico de hallazgos de auditoría y plan de mejoramiento a través del software.

11) **Conocimientos sobresalientes en Gestión de Riesgos y Diseño de Controles**





El Software AUDIRISK

Qué es y para que sirve?

Es un software en tecnología WEB (Cloud Computing) para ***conducir*** las siguientes actividades de la Auditoría Interna y de Sistemas, con un **enfoque PROACTIVO Y PREVENTIVO:**

1) **Elaborar el Plan Anual de Auditoría**, basado en "la Exposición a Riesgos" de los elementos del *Universo de Auditoría en la Empresa*.

2) **Desarrollar Auditorías "Basadas en Riesgos Críticos"** a los procesos del Modelo de Operación y los Servicios de Sistemas de la Empresa (Procesos del Área de TICs y Aplicaciones de Computador).

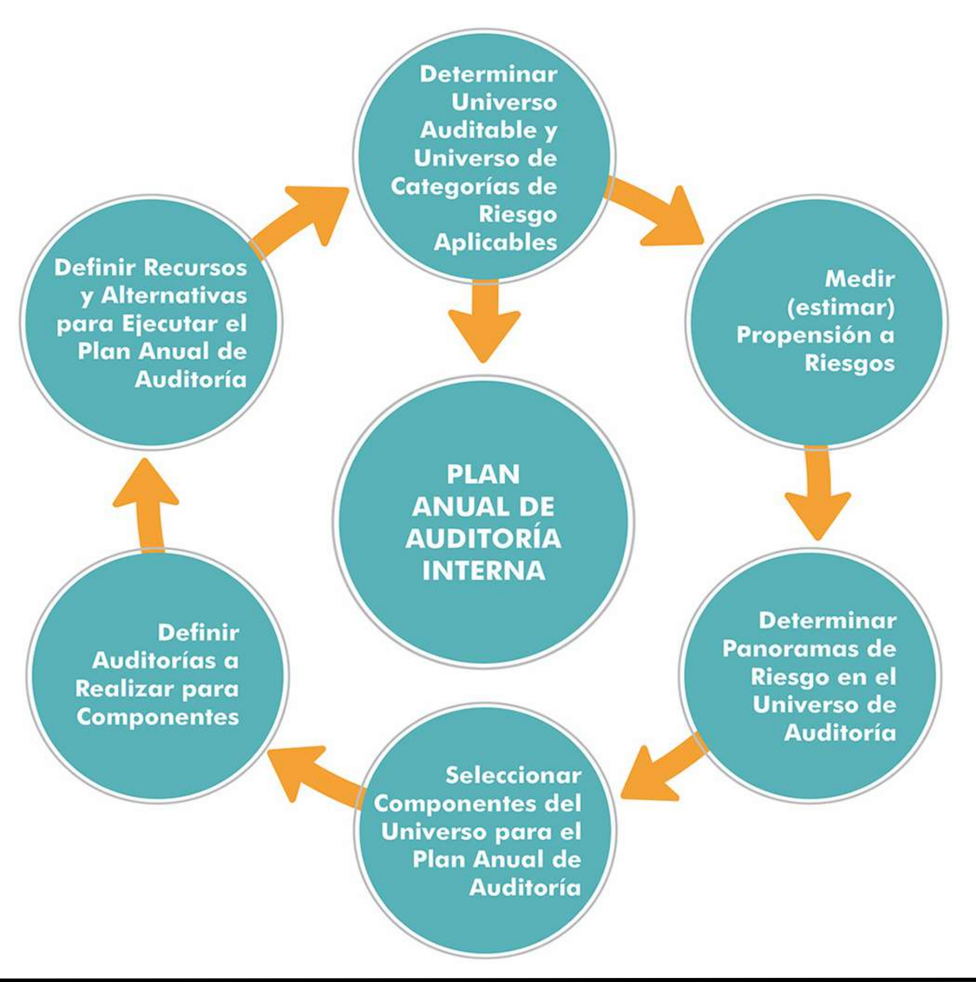
3) **Seguimiento de hallazgos de las Auditorías y a Planes de Mejoramiento**

4) **Gestión de la Auditoría**.

De conformidad con las normas y procedimientos de auditoría generalmente aceptados, las normas de auditoría interna del Instituto de Auditores Internos (IIA) y las normas de auditoría de sistemas de la Asociación de Control y Auditoría de Sistemas (ISACA).



Planeación Anual de Auditoría Interna “Basada en la Exposición a Riesgos”



AudiRisk:

- Conduce la elaboración del Plan de trabajo Anual de la auditoría interna, basado en resultados de “Valorar la “Exposición a riesgos, realizada al menos anualmente.
- Ayuda en la Comunicación y Aprobación del plan y los requerimientos de recursos para la actividad de Auditoría Interna.



Planeación Anual de Auditoría Interna "Basada en la Exposición a Riesgos"



Marco Internacional para la Practica Profesional de la Auditoría Interna.

- 2010. A1 - El plan de trabajo de la actividad de auditoría interna debe estar basado en una evaluación de riesgos documentada, realizada al menos anualmente. En este proceso deben tenerse en cuenta los comentarios de la alta dirección y del consejo.
- 2020 – Comunicación y Aprobación.

El auditor debe comunicar los planes y requerimientos de recursos de la actividad de Auditoría Interna, incluyendo los cambios provisionales significativos, a la alta dirección y al consejo para la adecuada revisión y aprobación y comunicar el impacto de cualquier limitación de recursos.



Planeación Anual de la Auditoría Interna, Basada en la Exposición a Riesgos

Entregables de la Planeación Anual de la Auditoría Interna.

1) **Elementos del Universo de Auditoría Interna de la Empresa considerados para valorar "Exposición a riesgos":** a) Inventario de procesos del modelo de operación; b) Inventario de procesos de TI; y c) Inventario de Aplicaciones de computador que soportan el core del negocio.

2) **Universo de Categorías de Riesgos** que pueden presentarse en las operaciones de la Empresa. Por ejemplo: Estratégico, Reputacional, SARO, SARLAFT, Financieros.
   SARO (7 categorías): Fraude interno, fraude externo, daños a activos físicos, fallas en atención a los clientes, problemas laborales, fallas tecnológicas y errores en la ejecución del proceso.
   SARLAFT: (4 categorías): Operativos, de Contagio, Reputacional y Legal (de Cumplimiento).





Planeación Anual de la Auditoría Interna, Basada en la Exposición a Riesgos

Entregables de la Planeación Anual de la Auditoría Interna.

3) **Cuestionarios para Estimar la Exposición a riesgos potenciales del Universo de Auditoría – Con Factores de Riesgo (preguntas) y Opciones de respuesta.**

- **TRES (3) cuestionarios**: Procesos del Modelo de Operación, Procesos de la infraestructura de TI y Aplicaciones de Computador o ERPs.

4) **Resultados del Procesamiento de los Cuestionarios:** Un puntaje entre 0 y 100 por cada elemento del Universo de Auditoría (proceso o sistema).



AUDIRISK

Planeación Anual de la Auditoría Interna, Basada en la Exposición a Riesgos

Entregables de la Planeación Anual de la Auditoría Interna.

5) **Matrices de Exposición a Riesgos, por Grupo de Elementos del Universo de Auditoría :**

   a) **Procesos Modelo de Operación Vs Categorías de Riesgo:** Priorización de procesos y de las categorías de riesgo dentro del Grupo procesos del modelo de operación,.
   b) **Procesos de Tecnología de Información Vs. Categorías de Riesgo:** Priorización de los procesos de TI y de las categorías de riesgo dentro del Grupo procesos de TI.
   c) **Aplicaciones de Computador Vs. Categorías de Riesgo:** Priorización de las Aplicaciones y de las categorías de Riesgo dentro del Grupo de elementos Aplicaciones .



Planeación Anual de la Auditoría Interna, Basada en la Exposición a Riesgos

Entregables de la Planeación Anual de la Auditoría Interna.

6) **Panoramas de Riesgo para los procesos del Modelo de Operación de la Empresa (Estratégicos, Misionales, de Soporte):**

   a) **Panorama de Riesgos Nivel 1:** Priorización de las categorías de riesgo dentro del Grupo procesos del modelo de operación.
   b) **Panorama de Riesgos Nivel 2:** Priorización de las categorías de riesgo dentro de cada proceso.
   c) **Perfiles de Riesgo por Categoría de Riesgo:** Exposición a cada categoría de Riesgo, de los procesos del Modelo de Operación.





Planeación Anual de la Auditoría Interna, Basada en la Exposición a Riesgos

Entregables de la Planeación Anual de la Auditoría Interna.

7) **Panoramas de Riesgo para los procesos de Tecnología de Información de la Empresa.**

8) **Panoramas de Riesgo para las Aplicaciones de Computador de Computador que soportan el Core del Negocio de la Empresa.**

9) **Elementos del Universo de Auditoria clasificados de mayor a menor Porcentaje de exposición a riesgos:** a) Procesos del Modelo de Operación; b) Procesos de TI; y c) Aplicaciones de Computador.





Planeación Anual de la Auditoría Interna, Basada en la Exposición a Riesgos

Entregables de la Planeación Anual de la Auditoría Interna.

10) **Programación de Trabajos de Auditoría para Elementos del Universo de Auditoría incluidos en el Plan Anual:** Fechas iniciación y terminación, horas estimadas, auditores asignados.

- **Trabajos Tipo 1**: Auditoría a un proceso o sistema, hasta Evaluación del Control Interno.
- **Trabajos Tipo 2**: Pruebas de Auditoría a un (1) proceso o sistema en Múltiples Sitios de Operación.
- **Trabajos Tipo 3:** Pruebas de Auditoría a Múltiples (varios) procesos o sistemas en un (1) Sitio de Operación.





Planeación Anual de la Auditoría Interna, Basada en la Exposición a Riesgos

Entregables de la Planeación Anual de la Auditoría Interna *(Cont.)*

11) **Gráfico de Barras –** Diagrama de Gantt con la programación anual y mensualizada de auditorías a realizar**.**

12) **Documento del Plan Anual de Auditoría:** para la Dirección de la Empresa y el Comité de Auditoría.

13) **Papeles de Trabajo de la Planeación Anual de la Auditoría -** Digitales y en Reportes.





El Software AUDIRISK

Qué es y para que sirve?

Es un software en tecnología WEB (Cloud Computing) para ***conducir*** las siguientes actividades de la Auditoría Interna y de Sistemas, con un **enfoque PROACTIVO Y PREVENTIVO:**

1) **Elaborar el Plan Anual de Auditoría**, basado en "la Exposición a Riesgos" de los elementos del *Universo de Auditoría en la Empresa*.
2) **Desarrollar Auditorías "Basadas en Riesgos"** a los procesos del Modelo de Operación y los Servicios de Sistemas de la Empresa (Procesos del Área de TICs y Aplicaciones de Computador).
3) **Seguimiento de hallazgos de las Auditorías y a Planes de Mejoramiento**
4) **Gestión de la Auditoría**.

De conformidad con las normas y procedimientos de auditoría generalmente aceptados, las normas de auditoría interna del Instituto de Auditores Internos (IIA) y las normas de auditoría de sistemas de la Asociación de Control y Auditoría de Sistemas (ISACA).





Desarrollo de Auditorías Basadas en Riesgos

Auditoria Basada en Riesgos

Requerimiento del negocio y de seguridad

Por cada
Proceso ó Sistema

1 Planeación basada en riesgos

2 Ejecución
- Evaluar Controles Establ.
- Pruebas de cumplimiento
- Pruebas sustantivas

3 Comunicación de resultados

4 Seguimiento

✓ Dictamen satisfacción requerimientos del negocio y de seguridad

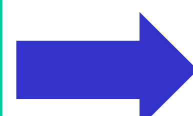




Enfoque de Auditoría “Basadas en Riesgos Críticos”

Qué es “Auditoría Basada en Riesgos Críticos”

*“Es una forma de conducir auditorías de diferentes tipos (operativa, de estados financieros, de sistemas de información, de sistemas de gestión), **CON ENFOQUE PROACTIVO Y PREVENTIVO**, basando su planeación y desarrollo en **una muestra de riesgos inherentes negativos,** que **pudieran causar daños o pérdidas significativas de activos** en los procesos o sistemas y la actividad económica de una organización, para confirmar que los procedimientos, controles y la información se ajustan a lo fijado por las leyes, las reglas del negocio y las buenas y mejores prácticas de control interno y seguridad”.*



***Por cada auditoría,** la revisión de los procedimientos, controles e información, incluye:*

- *Análisis de riesgos Inherentes de la muestra de auditoría,*
- *Evaluación del diseño y efectividad de controles establecidos,*
- *Diseño y ejecución de pruebas de auditoría (de cumplimiento y sustantivas),*
- *Generación de informes con los resultados de la auditoría y*
- *Seguimiento a Hallazgos de Auditoría y al Plan de Mejoramiento.*



AUDIRISK

Auditoría por Procesos “Basada en Riesgos”

Proceso:________________________________

PRE-AUDITORÍA	COMPRENSIÓN	MUESTRA DE RIESGOS INHERENTES	VALORAR SEVERIDAD DE RIESGOS (*)	EVALUAR CONTROL INTERNO	PRUEBAS DE CUMPLIMIENTO	PRUEBAS SUSTANTIVAS	INFORME CON RESULTADOS DE LA AUDITORÍA
		1	si	Satisfactorio	SI	?	SI
		2	si	Satisfactorio	SI	?	SI
		3		No Satisfactorio	NO	SI	SI
		. . .		.	.	.	.
		30	si	No Satisfactorio	NO	SI	SI

PLANEACION DETALLADA DE LA AUDITORIA “BASADA EN RIESGOS”

EVALUAR DISEÑO Y EFECTIVIDAD

PROGRAMA DE AUDITORÍA (Diseño, Planeación y Ejecución de Pruebas)

COMUNICACIÓN DE RESULTADOS Y SEGUIMIENTO

(*) E: Extremo; A: Alto; M: Moderado; B: Bajo





El Proceso de Auditoría "Basada en Riesgos"

Articulación Plan de Auditoría con Desarrollo de Auditorias Basadas en Riesgos

Planeación Anual Basada en Riesgos.

- ❑ Auditorias a realizar en el año.
- ❑ Categorías de riesgo críticas por componente.

Proceso de Auditoría "Basada en Riesgos Críticos"

Pre-auditoria y Familiarización con del proceso o sistema

- ❖ Memorando de planeación.
- ❖ Actualización de archivo permanente

Identificación y Análisis Riesgos Inherentes.
Eventos/Amenazas que pueden presentarse (20-30)

- E: Extremo
- A: Alto
- M: Moderado
- B: Bajo

Cubo de riesgos

Ejecución Auditoría

- ❖ Evaluación control Interno.
- ❖ Pruebas de Cumplimiento
- ❖ Pruebas sustantivas.

Informes con Resultados de la Auditoría.

- ❖ Evaluación control Interno.
- ❖ Pruebas de Cumplimiento
- ❖ Pruebas sustantivas.

Seguimiento a hallazgos de Auditoría

- ❖ Evaluación control Interno.
- ❖ Pruebas de Cumplimiento
- ❖ Pruebas sustantivas.



Cubo de Riesgos del Proceso o Sistema de Información objeto de Auditoría

Riesgos Inherentes

Areas Organiz y Terceros

Contabilidad

Recursos Humanos

Sistemas

Ingreso de Datos

Actualización Base de Datos

Reportes de Actualización

Fraude

Sanciones Legales

Costos Excesivos

Cat Riesgos Críticos

Actividades del Proceso (Escenarios de Riesgo)



AUDIRISK

Metodología de Auditoría Basada en Riesgos



1. **Pre-auditoría**
   - Memorando de Planeación
   - Programa de Trabajo

2. **Comprensión**
   - Archivo Permanente
   - Caracterización

3. **Id., y Análisis de Riesgos**
   - Muestra Riesgos Inherentes
   - Mapa de Calor o Mapa de Riesgos

4. **Contexto de Riesgos del Proceso**
   - Cubo de Riesgos proceso s. a. Auditoria



Etapas de la Auditoría "Basada en Riesgos Críticos"

FASES 2, 3 y 4: EJECUCION E INFORME DE LA AUDITORIA

5
Evaluar Controles Establecidos
- Evaluar Diseño y Efectividad
- Medir / evaluar Riesgo Residual
- Informe – Evaluación Control Interno

6
Pruebas de Cumplimiento
- % Cumplim. Cont. y Proced. Claves
- Informes Pruebas de Cumplimiento

7
Pruebas Sustantivas
- A Exactitud Cifras Claves
- Informes Pruebas Sustantivas

8
Seguimiento Hallazgos Informes de Auditoría
- Informe Estado Acciones de Mejora





Desarrollo de Auditorías Basadas en Riesgos

Tipos de Auditorías que puede Realizar con AUDIRISK .

1) A Procesos del Modelo de Operación de la Empresa – Componentes del Mapa de Procesos.
2) A Procesos de Tecnología de Información (TI): Procesos de Soporte y Suministro de Servicios
3) A las Aplicaciones de Computador o Módulos de ERPs que soportan el Core del Negocio.
4) A la Infraestructura de Tecnología de Informacion (Controles Generales de TI)



AUDIRISK

Desarrollo de Auditorías Basadas en Riesgos

Trabajos de Auditoría que puede realizar con AUDIRISK:

1. Auditoría a un proceso o Aplicación de Computador, hasta Evaluación del Control Interno.

2. Pruebas de Auditoría a un (1) proceso o Aplicación de Computador, en Múltiples Sitios de Operación.

3. Pruebas de Auditoría a Múltiples (varios) procesos o Aplicaciones de Computador, en un (1) Sitio de Operación.



Entregables de la Auditoría Basada en Riesgos

1. De la Auditoría de un Proceso o Sistema, hasta Evaluación del Control Interno:

1) Memorando de Planeación de la Auditoría .
2) Comprensión del Contexto Interno y Externo del Proceso – Archivo Permanente y Caracterización del proceso.
3) Categorías de Riesgo Críticas Aplicables al Proceso.
4) Cuestionario de riesgos potenciales para identificar Riesgos Inherentes que pueden generar las Categorías de Riesgo Críticos del Proceso
5) Selección de ***Muestra de Riesgos Inherentes para el desarrollo de la Auditoría – Máximo 30, mínimo 18***.
6) Documentación del Análisis de Riesgos Inherentes de la Muestra de Auditoría .
7) Mapas de Riesgos Inherentes y reportes de Análisis de Riesgos.
8) Opciones de manejo de riesgo seleccionadas por los Auditores para los riesgos de la muestra de auditoría (asumir, evitar, mitigar, transferir, distribuir)

.





Entregables de la Auditoría Basada en Riesgos

1. *De la Auditoría de un Proceso o Sistema, hasta Evaluación del Control Interno (Cont.)*

9) Documentación del Cubo de Riesgos del proceso objeto de la auditoria.
10) Objetivos de control que deberían satisfacerse para el proceso.
11) **Cuestionario de Controles "Que deberían Existir"** para los riesgos inherentes de la muestra de auditoría – *Sugeridos por el sistema y Enriquecidos por el Auditor.*
12) Identificación de Controles "Establecidos ó existentes", para los riesgos inherentes de la muestra de auditoría.
13) Resultados de Evaluación de la **Efectividad Individual y Colectiva** de los controles establecidos por Riesgo Inherente. – Incluye los Hallazgos de Auditoría.
14) Mapa de Riesgos Residuales, después de evaluar Efectividad de los controles.
15) *Informe con los Resultados de Auditoría a la Evaluación del Control Interno del proceso o sistema.*





Entregables de la Auditoría Basada en Riesgos

1. De la Auditoría de un Proceso o Sistema, hasta Evaluación del Control Interno (Cont):

16) Asignación de fechas limite para atender hallazgos de auditoría de evaluación del Control Interno y asignación de cargos responsables de atenderlos.

17) Correos electrónicos de notificación generados y enviados a los AUDITADOS sobre "Designación para atender hallazgos de Auditoria y asignación credenciales de acceso al software ".

18) Papeles de Trabajo Corrientes – Etapas 1 a 5 del proceso de Auditoría





Entregables de la Auditoría Basada en Riesgos

2. De las Pruebas de Cumplimiento a un (1) Proceso en Múltiples Sitios de Operación.

1) Memorando de Planeación de las Pruebas de Auditoría.
2) Diseño y Planeación de las Pruebas de Cumplimiento
3) Controles a verificar para los riesgos inherentes de la muestra de auditoría con resultados "Satisfactorios" en Evaluación de Control Interno.
4) Checklists de controles a verificar para riesgos inherentes con controles satisfactorios, por sitios de Operación y técnica de verificación.
5) Resultados de aplicar los Checklists de Controles en sitios de operación
6) Reportes generados por AUDIRISK con resultados de las pruebas ejecutadas – Incluye los Hallazgos de Auditoría.
7) Informe de Auditoría con los Resultados de las Pruebas de Cumplimiento, por sitios de prueba y consolidados por áreas organizacionales.





Entregables de la Auditoría Basada en Riesgos

2. De las Pruebas de Cumplimiento a un (1) Proceso en Múltiples Sitios de Operación (Cont).

8) Asignación fechas límite para atender hallazgos de auditoría de pruebas de cumplimiento y asignación de cargos responsables de atenderlos.
9) Correos electrónicos de notificación generados y enviados a los AUDITADOS sobre "Designación para atender hallazgos de Auditoria y asignación credenciales de acceso al software ".
10) Papeles de Trabajo de la planeación y ejecución de pruebas de cumplimiento – Archivo de papeles corrientes.
11) Control de Tiempo de la Auditoría.





Entregables de la Auditoría Basada en Riesgos

3. De las Pruebas Sustantivas a un (1) Proceso en Múltiples Sitios de Operación.

1) Memorando de Planeación de las Pruebas de Auditoría.
2) Diseño y Planeación de las Pruebas Sustantivas
3) Cifras (Datos) a verificar para los riesgos inherentes de la muestra de auditoría, que presentan debilidades de control en la evaluación de control interno.
4) Checklists de "Cifras a Verificar" para riesgos inherentes con debilidades de control, por sitios de Operación y técnica de verificación.
5) Resultados de Aplicación de los Checklists en los sitios de operación
6) Reportes generados por AUDIRISK con resultados de las pruebas ejecutadas – Incluye los Hallazgos de Auditoría.
7) Informes de Auditoría con los Resultados de las Pruebas Sustantivas, por sitios de prueba y consolidados por áreas organizacionales.





Entregables de la Auditoría Basada en Riesgos

3. De las Pruebas Sustantivas a un (1) Proceso en Múltiples Sitios de Operación (Cont).

8) *Informe con Resultados de la Evaluación de los siete (7) criterios que debe satisfacer la información de negocios.*
9) Asignación fechas limite para atender hallazgos de auditoría de pruebas sustantivas y cargos responsables de atenderlos.
10) Correos electrónicos de notificación generados y enviados a los AUDITADOS sobre "Designación para atender hallazgos de Auditoria y asignación credenciales de acceso al software ".
11) Papeles de Trabajo Corrientes de las Pruebas Sustantivas.
12) Control de Tiempo de la Auditoría.





Entregables de la Auditoría Basada en Riesgos

4. De las Pruebas de Cumplimiento a Múltiples Procesos en un (1) Sitio de Operación.

Por cada Proceso:

1) Memorando de Planeación de las Pruebas de Auditoría.
2) Diseño y Planeación de las Pruebas de Cumplimiento.
3) Controles a verificar para los riesgos inherentes de la muestra de auditoría con resultados "Satisfactorios" en Evaluación de Control Interno.
4) Checklists de controles a verificar para riesgos inherentes con debilidades de control, por sitios de Operación y técnica de verificación.
5) Resultados de aplicar los Checklists de Controles en el sitio de operación
6) Reportes generados por AUDIRISK con resultados de las pruebas ejecutadas – Incluye los Hallazgos de Auditoría.
7) Informe de Auditoría con los Resultados de las Pruebas de Cumplimiento del proceso en el sitios de operación.





Entregables de la Auditoría Basada en Riesgos

4. De las Pruebas de Cumplimiento a Múltiples Procesos en un (1) Sitio de Operación (Cont).

Por cada proceso

8) Asignación fechas límite para atender hallazgos de auditoría de pruebas de cumplimiento y asignación de cargos responsables de atenderlos.
9) Correos electrónicos de notificación generados y enviados a los AUDITADOS sobre "Designación para atender hallazgos de Auditoria y asignación credenciales de acceso al software ".
10) Papeles de Trabajo de las pruebas de cumplimiento al Proceso – Archivo de papeles corrientes.
11) Control de Tiempo de la Auditoría.

De todos los procesos revisados en el Sitio

12) Informe Consolidado con los resultados de las pruebas de cumplimiento.





Entregables de la Auditoría Basada en Riesgos

5. De las Pruebas Sustantivas a Múltiples Procesos en un (1) Sitio de Operación.

Por cada proceso.

1) Memorando de Planeación de las Pruebas de Auditoría.
2) Diseño y Planeación de las Pruebas Sustantivas
3) Cifras (Datos) a verificar para los riesgos inherentes de la muestra de auditoría, que presentan debilidades de control en la evaluación de control interno.
4) Checklists de "Cifras a Verificar" para riesgos inherentes con debilidades de control, por sitios de Operación y técnica de verificación.
5) Resultados de Aplicación de los Checklists en los sitios de operación
6) Reportes generados por AUDIRISK con resultados de las pruebas ejecutadas – Incluye los Hallazgos de Auditoría.
7) Informes de Auditoría con los Resultados de las Pruebas Sustantivas del proceso en el sitio de operación.





Entregables de la Auditoría Basada en Riesgos

5. De las Pruebas Sustantivas a Múltiples Procesos en un (1) Sitio de Operación (Cont).

Por cada proceso

8) *Informe con Resultados de la Evaluación de los siete (7) criterios que debe satisfacer la información de negocios.*
9) Asignación fechas limite para atender hallazgos de auditoría de pruebas sustantivas y cargos responsables de atenderlos.
10) Correos electrónicos de notificación generados y enviados a los AUDITADOS sobre "Designación para atender hallazgos de Auditoria y asignación credenciales de acceso al software ".
11) Papeles de Trabajo Corrientes de las Pruebas Sustantivas.
12) Control de Tiempo de la Auditoría.

De todos los procesos revisados en el Sitio

13) Informe Consolidado con los resultados de las Pruebas Sustantivas.





El Software AUDIRISK

Qué es y para que sirve?

Es un software en tecnología WEB (Cloud Computing) para ***conducir*** las siguientes actividades de la Auditoría Interna y de Sistemas, con un **enfoque PROACTIVO Y PREVENTIVO:**

1) **Elaborar el Plan Anual de Auditoría**, basado en "la Exposición a Riesgos" de los elementos del *Universo de Auditoría en la Empresa*.

2) **Desarrollar Auditorías "Basadas en Riesgos Críticos"** a los procesos del Modelo de Operación y los Servicios de Sistemas de la Empresa (Procesos del Área de TICs y Aplicaciones de Computador).

3) **Seguimiento de hallazgos de Auditorías y Planes de Mejoramiento**

4) **Gestión de la Auditoría**.

De conformidad con las normas y procedimientos de auditoría generalmente aceptados, las normas de auditoría interna del Instituto de Auditores Internos (IIA) y las normas de auditoría de sistemas de la Asociación de Control y Auditoría de Sistemas (ISACA).

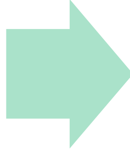




El Software AUDIRISK

Qué es y para que sirve?

Seguimiento a Hallazgos de Auditoría y Acciones de Mejoramiento.



- El software provee acceso a los auditados, por cada auditoría, para ingresar planes de acción por hallazgo y avances de implantación.
- Generación y envío automático de Correos Electrónicos de Recordatorio, a responsables de implantar, supervisar y hacer seguimiento a acciones de mejora.
- Genera estadísticas del estado de implantación de las acciones de mejora (implantadas, en proceso, pendientes de atender, anulados).





El Software AUDIRISK

Qué es y para que sirve?

Es un software en tecnología WEB (Cloud Computing) para ***conducir*** las siguientes actividades de la Auditoría Interna y de Sistemas, con un **enfoque PROACTIVO Y PREVENTIVO:**

1) **Elaborar el Plan Anual de Auditoría**, basado en "la Exposición a Riesgos" de los elementos del *Universo de Auditoría en la Empresa*.
2) **Desarrollar Auditorías "Basadas en Riesgos Críticos"** a los procesos del Modelo de Operación y los Servicios de Sistemas de la Empresa (Procesos del Área de TICs y Aplicaciones de Computador).
3) **Seguimiento de hallazgos de las Auditorías y a Planes de Mejoramiento**
4) **Gestión de la Auditoría.**

De conformidad con las normas y procedimientos de auditoría generalmente aceptados, las normas de auditoría interna del Instituto de Auditores Internos (IIA) y las normas de auditoría de sistemas de la Asociación de Control y Auditoría de Sistemas (ISACA).

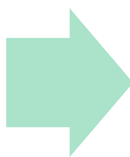




El Software AUDIRISK

Qué es y para que sirve?

Generar Informes con indicadores de Gestión de la Auditoría.



Informes de Gestión de la Auditoría. Estadísticas y gráficos de Auditorías realizadas:

- Hallazgos de Auditoría: Control Interno (CI), pruebas de Cumplimiento (PC) y pruebas Sustantivas (PS).
- Recomendaciones Emitidas: CI; PC; PS.
- Estado de las Recomendaciones.
- Auditorías Programadas y Ejecutadas.
- Horas Cargables por Auditoría y Auditor.
- Costos por Auditoría y Auditor.





Agenda

- AudiRisk: Qué es y para Qué Sirve?.
- **Características del Software AudiRisk que agregan valor a las Organizaciones y las Auditorías.**
- Especificaciones Técnicas del Software AudiRisk.
- Requerimientos de Hardware y Software para instalar AUDIRISK.
- Productos que recibe el Usuario de AUDIRISK.
- Beneficios de Utilizar AudiRisk.
- Usuarios del software AudiRisk.





Propuesta de valor del Software AUDIRISK.

Valor Percibido para las Empresas Usuarias

1) *El software es multiempresa,* es decir, permite realizar planeación anual, auditorías y seguimientos para múltiples empresas, con la misma cantidad de usuarios para todas las empresas. Con las mismas credenciales y el mismo perfil, un usuario puede realizar auditorías a múltiples empresas.

2) Provee una metodología sencilla y efectiva para elaborar el Plan Anual de Auditoría Interna***, "basado en la valoración de la exposición a riesgos" en los componentes del Universo de Auditoría.***

3) *Las Auditorías se ejecutan con enfoque PROACTIVO Y PREVENTIVO* para **evaluar y verificar** que los procesos y sistemas de la empresa sean eficaces, eficientes y seguros; es decir, que satisfacen los objetivos de empresa y están adecuadamente protegidos contra los eventos de riesgo críticos que pudieran presentarse en el desarrollo de las operaciones.





Propuesta de valor del Software AUDIRISK.

Valor Percibido para las Empresas Usuarias

4) Se desarrollan las cuatro (4) fases del proceso de auditoría ***"basándose en una muestra de eventos de riesgo inherentes Críticos",*** *que representan los riesgos de mayor impacto para la organización.*

5) El software ***genera los Archivos de Papeles de Trabajo en formato electrónico (archivo permanente y archivo de papeles de trabajo corrientes)*****.** El software AUDIRISK, en cada una de las siete etapas del proceso de Auditoría Basada en Riesgos, genera los papeles de trabajo de la auditoría en formato electrónico y exportables a PDF y otros formatos.

6) AUDIRISK provee funcionalidades **de mensajería interna (TO DOs) y correos electrónicos para interacción entre Auditores y Auditados**, en aspectos de planeación y ejecución del seguimiento de hallazgos de auditoria, la aprobación del plan de mejoramiento y seguimiento a la implantación de acciones de mejora.

.





Propuesta de valor del Software AUDIRISK.

Valor Percibido para las Empresas Usuarias

7. ***Provee funcionalidades para elaborar cuestionarios y Checklists (CSAs: Control Self Assessment). Estos no son insumos, son productos de AudiRisk:***
   - ❑ Para estimar la exposición a riesgos de los procesos y sistemas de la organización – Del Universo de Auditoría.
   - ❑ Para identificar y seleccionar los eventos de riesgos inherentes (amenazas) para las tres o cuatro categorías de riesgos críticas, que serán considerados por el alcance de las auditorías.
   - ❑ Para identificar los controles que "deberían existir" y los "controles establecidos" para los eventos de riesgo (amenazas) considerados en alcance de las auditorías
   - ❑ Para verificar los controles (pruebas de cumplimiento) de amenazas que tienen protección apropiada.
   - ❑ Para verificar la exactitud de la información (pruebas sustantivas) a cifras impactadas por eventos de riesgo (amenazas) con debilidades de control.
   - ❑ Para evaluar la satisfacción de las siete (7) características de las información de negocios.





Propuesta de valor del Software AUDIRISK.

Valor Percibido para las Empresas Usuarias

8) *Cada auditoría evalúa el estado de la "Cultura de Riesgos y Controles" existente en la Empresa y estimula (potencia) a los auditores para **actuar como "Agentes de Cambio"** de la cultura existente.*

9) *Verifica que los controles por cada evento de riesgo inherente, **satisfagan dos requisitos para ser eficaces:*** a) Eliminan las vulnerabilidades y b) bloquean o neutralizan los agentes generadores del riesgo.

10) *Aplica y promueve la implantación del enfoque de los **"tres anillos de seguridad o Líneas de defensa"** y del **nivel de automatización y no discrecionalidad de los controles**, como criterios para evaluar la EFICACIA de los controles establecidos sobre los riesgos inherentes.*

11) Evalúa que sea RAZONABLE la relación COSTO /BENEFICIO de los controles establecidos por cada evento de riesgo inherente, como criterio para evaluar la EFICIENCIA de los controles.



Propuesta de valor del Software AUDIRISK.

Valor Percibido para las Empresas Usuarias.

12) ***Lo que no se puede medir, no se puede administrar.*** Utiliza una escala numérica para CALIFICAR la **Efectividad (Eficacia + eficiencia)** de los controles por evento de riesgo inherente, en Evaluación del Control Interno y Pruebas de auditoría: 5**- Apropiada, 4-Mejorable, 3-Insufiicente, 2- Deficiente y 1- Muy deficiente.**

13) ***Lo que no se puede medir, no se puede administrar.*** Utiliza una escala para CALIFICAR el **Riesgo Residual** por evento de riesgo inherente, después de realizar la Evaluación del Control Interno y Ejecutar las Pruebas de Auditoría: **1- Bajo (Tolerable), 2-Moderado, 3- Alto y 4: Extremo.**

14) Diseña y Ejecuta las pruebas de cumplimiento y sustantivas de acuerdo con los resultados de la Evaluación de Control Interno (Aplica la Segunda Norma de Auditoría relativa a la Ejecución del Trabajo).





Propuesta de valor del Software AUDIRISK.

Valor Percibido para las Empresas Usuarias

15) Con los resultados de las pruebas de cumplimiento y sustantivas, la auditoría **mide porcentualmente (%) el cumplimiento de los controles establecidos y de la exactitud de la información**, por cada riesgo inherente de la muestra de auditoría, *para presentar el estado de severidad real de los riesgos residuales que esta asumiendo la organización*.

16) Provee funcionalidades para generar y conservar todos los papeles de trabajo de las auditorías en formato electrónico (archivos permanentes y archivos corrientes).

17) Provee funcionalidades para elaborar el plan de mejoramiento que resulta de los hallazgos de las auditorías, planear su implantación y ejecutar el seguimiento. Genera correos electrónicos recordatorios para los responsables de implantar, supervisar la implantación y efectuar el seguimiento a las acciones de mejora.





Propuesta de valor del Software AUDIRISK.

Valor Percibido para las Empresas Usuarias

18) El enfoque Basada en Riesgos, facilita la transición de los auditores, del estado *“ser y actuar como consumidores de conocimientos”* a convertirse en *“generadores de conocimiento y de valor para las organizaciones”.*

19) El enfoque Basada en Riesgos, **contribuye a superar algunas Críticas a la Auditoría.**

   a) Históricamente se les conoce por su habilidad para encontrar fallas en el trabajo de los auditados – ***El Auditor Investigador y Acusador*.**
   b) *Promueve la Cultura de priorización en la Auditoría.* “Por estar cuidando las hormigas, se dejan pasar los Elefantes…” **POR QUE?.**
   c) *Desestimula la* ***Controlitis Aguda.*** *Evalúa el diseño y el C/B (la eficiencia) de los Controles, cuando se recomiendan controles.*
   d) Desestimula la Inoportunidad de las Recomendaciones: *Las revisiones y consejos llegan tarde – Después de la ocurrencia de los riesgos / problemas.*
   e) Desestimula el enfoque Reactivo de la Auditoría: Algunas veces, l*os Auditores actúan como los “Bomberos”.*





Propuesta de valor del Software AUDIRISK.

Valor Percibido para las Empresas Usuarias

20) ***Utiliza modelos Universales de "clases o categorías de riesgo" como base para determinar el "Universo de Riesgos de la Empresa", planear y desarrollar las Auditorías.***

- ❑ Sistema de Administración de Riesgo Operativo- SARO.
- ❑ Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo - SARLAFT.
- ❑ MECI (Modelo Estándar de Control Interno para las Entidades del Estado Colombiano).
- ❑ Riesgos en el Sector Salud - Res 1740 de 2008 MPS.
- ❑ AUDIRISK.
- ❑ Otros Modelos (Basilea en Sector financiero y Sector Salud).





Propuesta de valor del Software AUDIRISK.

Valor Percibido para las Empresas Usuarias

21) "Lo que no se mide, no se puede administrar / Controlar". Por cada Auditoría:

- Evalúa y Mide la **Efectividad de los Controles Existentes,** por Evento de Riesgo Inherente (Amenaza), categorías de riesgo, actividades, áreas organizacionales y objetivos de control. 5**:** Apropiada, 4**:** Mejorable; **3:** Insuficiente; 2**:** Deficiente y **1**: Muy deficiente
- En las pruebas de Cumplimiento, mide el **% de Cumplimiento de los Controles Establecidos**, por amenazas, categorías de riesgo, actividades, áreas organizacionales.
- En las Pruebas Sustantivas, mide el **% de Exactitud de las Cifras verificadas**, por amenazas, categorías de riesgo, actividades, áreas organizacionales.
- Mide porcentualmente la satisfacción de los siete (7) criterios de la información de negocios.





Propuesta de valor del Software AUDIRISK.

Valor Percibido para las Empresas Usuarias

22) Otras características del software que generan valor.

- ⇨ Es una aplicación WEB que se puede instalar en la Nube (Cloud Computing), servidores de la empresa y equipos stand alone.
- ⇨ Software Multiempresa.
- ⇨ Produce Papeles de Trabajo en formato electrónico.
- ⇨ Ofrece ayudas de Supervisión de los Auditores (TO DOs o pendientes por hacer).
- ⇨ Por cada auditoría genera 5 tipos informes de Auditoria: Evaluación de control interno, pruebas de cumplimiento, pruebas sustantivas, satisfacción de las siete (7) características de la información de negocios y del seguimiento a los hallazgos de auditoría.
- ⇨ Deja Rastros de las actividades ejecutadas por los Auditores.
- ⇨ Genera indicadores de Gestión de la Auditoría.





El Software AUDIRISK

AUDIRISK está alineado y es compatible con estándares internacionales y nacionales vigentes de auditoría, gestión de riesgos, control interno y seguridad.

- ❑ Normas de Auditoría de Aceptación General.
- ❑ Normas de Auditoria Interna del IIA.
- ❑ Normas de Auditoría de Sistemas de ISACA.
- ❑ Modelos de Control Interno COSO 2013, COBIT Y MECI.
- ❑ Gestión de Seguridad de la Información: Normas ISO 27001.
- ❑ ISO 20000: Gestión de Servicios de TI.
- ❑ Otras ISO 9126, ISO 12207 e ISO 38500 (Gobierno de TI).
- ❑ Marcos de Referencia para Gestión de Riesgos: ISO 31000, ERM, SARO, SARLAFT, DAFP, SALUD.





El software AUDIRISK

Satisface necesidades de diferentes modalidades de Auditoría.

- ⇨ Auditores Internos
- ⇨ Auditores de Sistemas.
- ⇨ Auditores Operativos.
- ⇨ Auditores de Procesos.
- ⇨ Auditorías Integrales.
- ⇨ Revisores Fiscales.





Agenda

- AudiRisk: Qué es y para Qué Sirve?.
- Características del Software AudiRisk que agregan valor a las Organizaciones y las Auditorías.
- **Especificaciones Técnicas del Software y Requerimientos de Hardware y Software para instalar AUDIRISK.**
- Modalidades de Licenciamiento.
- Productos que recibe el Usuario de AUDIRISK.
- Presentación Detallada de los Módulos Componentes del Software AudiRisk.
- Beneficios de Utilizar AudiRisk.
- Usuarios del software AudiRisk.





Especificaciones Técnicas del Software AUDIRISK

- Herramienta de Desarrollo: .NET, Visual Studio.
- Sistema Operacional: Windows Server 2008 a 2012. Windows Vista, 7, 8 Y 10. Excepto las versiones Home.
- Motor de Base de datos: SQL Server.
- Memoria RAM: 4GB en servidor.
- Disco Duro: 16 GB.
- Navegadores: Internet Explorer 8.0 o superiores, Google Chrome, Firefox y Opera.





Agenda

- AudiRisk: Qué es y para Qué Sirve?.
- Características del Software AudiRisk que agregan valor a las Organizaciones y las Auditorías.
- Especificaciones Técnicas del Software y Requerimientos de Hardware y Software para instalar AUDIRISK.
- **Modalidades de Licenciamiento.**
- Productos que recibe el Usuario de AUDIRISK.
- Presentación Detallada de los Módulos Componentes del Software AudiRisk.
- Beneficios de Utilizar AudiRisk.
- Usuarios del software AudiRisk.





Modalidades de Licenciamiento del Software

Venta de Licencias a Perpetuidad

Licenciamiento a perpetuidad, por equipo (servidor) y cantidad de usuarios concurrentes.

a) De perfil AUDITOR: con acceso todas las funcionalidades del software.

b) De perfil Auditado: con acceso como Implantadores de Acciones de Mejora en el módulo de Seguimiento y con limitaciones a otros módulos del aplicativo.

El software se instala en un Hosting de la Empresa ó Comercial contratado por la empresa que adquiere las licencias de uso.





Modalidades de Licenciamiento del Software

Licenciamiento por Suscripcion Anual Arrendamiento Anual.

La Suscripción Anual se pacta por equipo (servidor) y cantidad de usuarios concurrentes.

a) De perfil AUDITOR: con acceso todas las funcionalidades del software.

b) De perfil Auditado: con acceso como Implantadores de Acciones de Mejora en el módulo de Seguimiento y con limitaciones a otros módulos del aplicativo.

El software se instala en un Servidor Web de la Empresa ó en un hosting Comercial contratado por la empresa que adquiere el servicio de suscripción anual





Agenda

- AudiRisk: Qué es y para Qué Sirve?.
- Características del Software AudiRisk que agregan valor a las Organizaciones y las Auditorías.
- Especificaciones Técnicas del Software AudiRisk.
- Requerimientos de Hardware y Software para instalar AUDIRISK.
- **Productos que recibe el Usuario de AUDIRISK.**
- Presentación Detallada de los Módulos Componentes del Software AudiRisk.
- Beneficios de Utilizar AudiRisk.
- Usuarios del software AudiRisk.





Entregables que recibe el Usuario de AUDIRISK

Por la compra de Licencias de Uso del Software

- ⇨ Manual del Usuario del Software (E-book).
- ⇨ Software ejecutable (DVD).
- ⇨ Bases de datos de conocimientos estándar.
- ⇨ Licencia de uso a perpetuidad, por servidor y cantidad de usuarios concurrentes.
- ⇨ Acceso a la Empresa ITF “Morraos de Colombia”, para consultar dos (2) Ejemplos de Auditorías Basadas en Riesgos Críticos y realizar pruebas con fines de capacitación y entrenamiento .
- ⇨ Derecho a recibir soporte técnico y actualizaciones del software y la metodología durante un año.



Entregables que recibe el Usuario de AUDIRISK

Por el Arrendamiento / Suscripcion Anual de Licencias de Uso del Software

- ⇨ Manual del Usuario del Software (E-book).
- ⇨ Acceso utilizar el Software ejecutable (CD) como empresa Licenciataria.
- ⇨ Acceso a Bases de datos de conocimientos estándar.
- ⇨ Acceso a la Empresa ITF “Morraos de Colombia”, para consultar dos (2) Ejemplos de Auditorías Basadas en Riesgos Críticos y realizar pruebas con fines de capacitación y entrenamiento .
- ⇨ Derecho a recibir soporte técnico y actualizaciones del software y la metodología durante un año.





Entregables que recibe el Usuario de AUDIRISK

Servicios Complementarios.

- Capacitación para la Operación del Software.
- Consultoría - Acompañamiento para Integrar el Software al proceso del "dia a dia" de la Auditoría. ***Por cada tema principal del software***, consta de 3 sesiones:
  - **Sesión 1:** Capacitación para el uso de la metodología y el software, por parte del Consultor.
  - **Sesión 2:** Trabajo de campo por los auditores de la Empresa, en Ejecución de Auditorías a procesos y sistemas.
  - **Sesión 3:** Retroalimentación por el consultor.
- Servicio Anual de Actualización y Soporte Técnico.





Agenda

- **AudiRisk: Qué es y para Qué Sirve?.**
- Características del Software AudiRisk que agregan valor a las Organizaciones y las Auditorías.
- Especificaciones Técnicas del Software AudiRisk.
- Modalidades de Licenciamiento.
- Entregables que recibe el Usuario de AUDIRISK.
- **Presentación detallada de los Módulos Componentes del Software AudiRisk.**
- Beneficios de Utilizar AudiRisk.
- Usuarios del software AudiRisk.





El Software AUDIRISK

Qué es y para que sirve?

Módulos del Software AUDIRISK.

Consta de seis (6) módulos interrelacionados:

1) Administración de Usuarios.
2) Parametrización / Configuración del Software.
3) Planeación Anual de la Auditoría (Interna ó Externa) Basada en Valoración de la Exposición a Riesgos.
4) Desarrollo de Auditorías "Basadas en Riesgos Críticos" para procesos y Servicios de Sistemas de Información.
5) Seguimiento a Hallazgos de Auditoría y Planes de Mejoramiento.
6) Gestion de Resultados de la Auditoría.





El Software AUDIRISK

1
Administración de Usuarios

Asignar Perfiles
Asignar Perfiles
Asignar Perfiles
Asignar Perfiles

3
Planeación Anual de la Auditoría Basada en Riesgos

Plan Anual de Auditoría

2
Parametrización del Software

Universo
Categorías de Riesgo
Universo Auditable

6
Gestión de Resultados de la Auditoría

Tipos de Allazgos

Plan Anual de Auditoría

Estándares de la Auditoría

4
Desarrollo Auditorías basadas en Riesgos Críticos

Hallazgos y Acciones de Mejora

5
Seguimiento a Hallazgos de Auditoría y Planes de Mejoramiento.

Módulos del Software AUDIRISK





El Software AUDIRISK

MODULO 1: Administración de Usuarios

- Asignar Perfiles de acceso.
- Asignación de Auditores a Auditorías.
- Cambio / inactivación de password.
- Copias de Seguridad (Backups).

Perfil Auditor - acceso al Software AUDIRISK

- Gerente de Auditoría.
- Supervisor de Auditoría.
- Analista de Auditoría (Auditor de Procesos o de Aplicaciones).
- Audito Regional.
- Comité de Auditoría .





El Software AUDIRISK

MODULO 1: Administración de Usuarios

- Asignar Perfiles de acceso.
- Asignación de Auditores a Auditorías.
- Cambio / inactivación de password.
- Copias de Seguridad (Backups).

Perfil Auditado - acceso al Software AUDIRISK

- Implantadores de Acciones de Mejora.
- Supervisores de Implantación de Acciones de Mejora.
- Auxiliar de implantación





Módulo 2: Parametrización del Software

Objetivos:

1. Dar Mantenimiento a la ***Base de Datos de "Conocimientos de Auditoría"*** suministrada por el proveedor (AUDISIS), antes de iniciar uso del software.

    - Categorías de Riesgo.
    - Eventos de Riesgo Inherentes por categoría de riesgo.
    - Controles por Evento de riesgo inherente.
    - Técnicas de auditoría.
    - Otras.

2. Cargar o poblar tablas con información privada específica de la Empresa licenciataria.

3. Definir parámetros para CALIFICAR (medir) la severidad del riesgo, efectividad de los controles, los resultados de pruebas de auditoría, severidad de los hallazgos de auditoría y otros.



El Software AUDIRISK

MODULO 2: Parametrización del Software

Configuración de los estándares de trabajo de las *Auditorías Basadas en Riesgos*.

Para Evaluar la efectividad de los controles establecidos.

Para evaluar resultados de pruebas de cumplimiento y sustantivas.

Para Evaluación satisfacción de los siete (7) criterios de la información de negocios (eficacia, eficiencia, integridad, disponibilidad, confidencialidad, confiabilidad y cumplimiento).

AudiRisk provee funcionalidades para ***configurar el correo electrónico corporativo de la Auditoría y enviar automáticamente mensajes de recordatorio dirigidos a:***

- Los responsables de implantar, supervisar la implantación y hacer seguimiento a las acciones de mejora por **hallazgos de control interno**.
- Responsables de implantar, supervisar la implantación y hacer seguimiento a las acciones de mejora por **hallazgos de Pruebas de Cumplimiento**.
- Responsables de implantar, supervisar la implantación y hacer seguimiento a las acciones de mejora por **hallazgos de Pruebas Sustantivas.**
- Responsables de implantar, supervisar la implantación y hacer seguimiento a las acciones de mejora **por hallazgos de Auditorías efectuadas por Terceros**.





Módulo 3:

Planeación Anual de la Auditoría, Basada en Valoración de Riesgos



Módulo 3: Planeación Anual de la Auditoría, Basada en Valoración de Riesgos

Objetivos:

1. Definir los trabajos de auditoría (nombre y alcance) que se ejecutarán durante el año, utilizando como criterio de selección el ***"Nivel de Exposición a Riesgos,*** para los elementos del Universo de Auditoría, es decir:

    a) Los procesos del modelo de operación de la empresa;
    b) Los procesos de la infraestructura de TIC, y
    c) Las Aplicaciones de Computador (módulos de ERPs) que soportan las operaciones criticas de la Empresa.

2. Definir los recursos de personal, tiempo, financieros y tecnológicos necesarios para ejecutar y cumplir el plan Anual de la Auditoría.

3. Generar "***documentos soportes de la Planeación Anual de la Auditoría",*** para consideración y aprobación de la Alta Dirección y el Comité de Auditoría.





El Software AUDIRISK

MODULO 3: Planeación Anual de la Auditoría, Basada en Valoración de la Exposición a Riesgos.

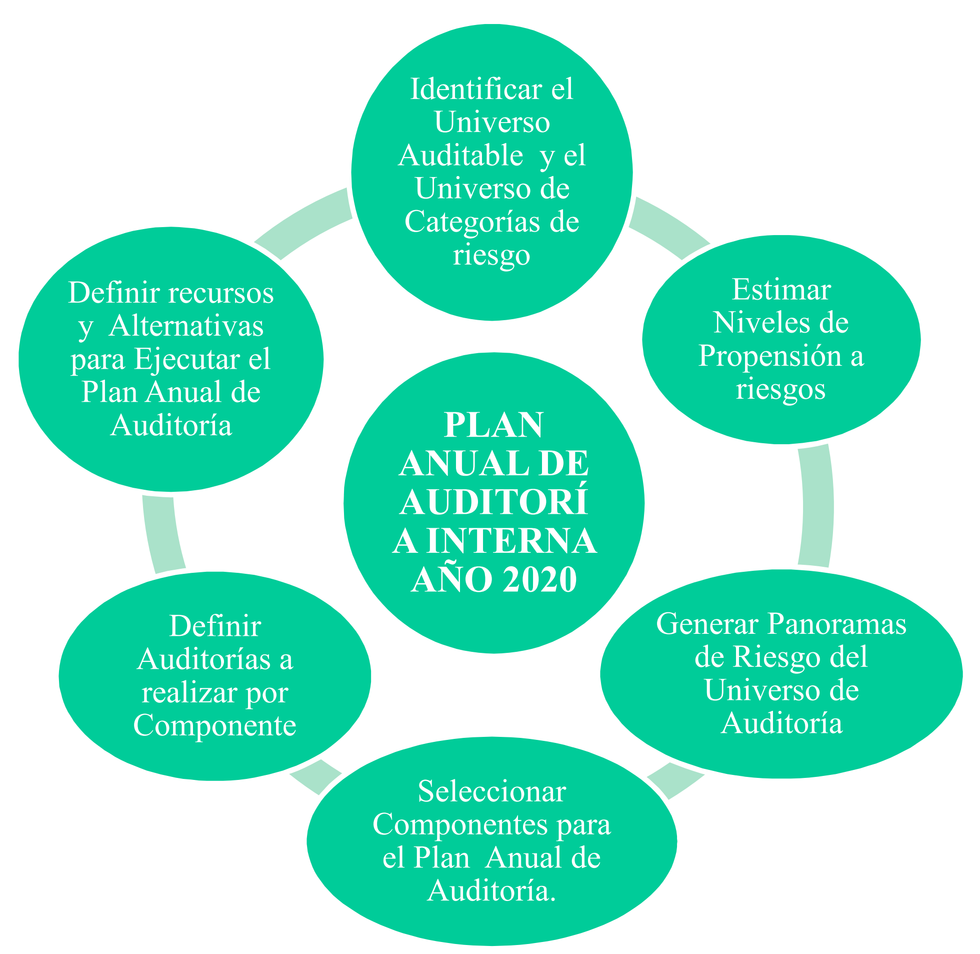
- Crear Ambiente de Trabajo.
- Procesar Cuestionarios.
- Elaborar Plan Anual de la Auditoría.
- Efectuar Seguimiento al desarrollo del Plan Anual.

Elaborar Plan Anual de la Auditoría :

- Seleccionar Trabajos que se incluirán en el Plan Anual de Auditoría, *los trabajos se seleccionarán de acuerdo al nivel de exposición a Riesgos*.
- Programar Trabajos de Auditoría.
- Generar el Plan Anual de Auditoría.



Pasos para Elaborar el Plan Anual de Auditoría Interna "Basado en Riesgos"



Marco Internacional para la Practica Profesional de la Auditoría Interna del IIA.

- 2010. A1-El plan de trabajo de la actividad de auditoría interna debe estar basado en una evaluación de riesgos documentada, realizada al menos anualmente. En este proceso deben tenerse en cuenta los comentarios de la alta dirección y del consejo.
- 2020 – Comunicación y Aprobación.

El auditor debe comunicar los planes y requerimientos de recursos de la actividad de Auditoría Interna, incluyendo los cambios provisionales significativos, a la alta dirección y al consejo para la adecuada revisión y aprobación y comunicar el impacto de cualquier limitación de recursos.





Planeación Anual de la Auditoría Interna, Basada en Exposición Riesgos”.

Pasos de la Metodología.

1. Identificar el Universo Auditable para la Auditoría Interna.

2. Identificar el Universo de Riesgos Aplicables a la Empresa





Identificar el Universo Auditable para Auditoría Interna

" Un conjunto finito y global de las áreas de auditoría, entidades organizacionales y la identificación y ubicación de las funciones de negocios que podrían ser auditadas para proporcionar un aseguramiento adecuado sobre el nivel de gestión de riesgos de la organización"

GTAG 11-The IIA Global





Identificar el Universo Auditable para Auditoría Interna

Inventario de:

1) Procesos del Modelo de Operación de la Empresa – Mapa de Procesos.
2) Aplicaciones de Computador o Módulos de ERPs.
3) Procesos de Tecnología de Información (TI): **Soporte y Suministro de Servicios de Sistemas**
4) Otros: trabajos de asesoría y aseguramiento.





Mapa de Procesos

ACTIVIDAD LITIGIOSA CONTRA EL ESTADO

PROCESOS ESTRATÉGICOS

- DIRECCIONAMIENTO ESTRATÉGICO
- INTELIGENCIA PARA LA DEFENSA JURÍDICA
- GESTIÓN CON GRUPOS DE INTERÉS Y COMUNICACIONES

PROCESOS MISIONALES

USUARIOS (ENTIDADES Y ORGANISMOS DEL ORDEN NACIONAL)

- GESTIÓN DE INFORMACIÓN DE DEFENSA JURÍDICA
- GESTIÓN DE PREVENCIÓN DEL DAÑO ANTIJURÍDICO
- GESTIÓN DEL CONFLICTO JURÍDICO
- GESTIÓN DE COMPETENCIAS INSTITUCIONALES PARA LA DEFENSA JURÍDICA

USUARIOS SATISFECHOS (ENTIDADES Y ORGANISMOS DEL ORDEN NACIONAL)

GESTIÓN DEL SISTEMA ÚNICO DE INFORMACIÓN LITIGIOSA DEL ESTADO

PROCESOS DE APOYO

- GESTIÓN DOCUMENTAL
- GESTIÓN DE TALENTO HUMANO
- GESTIÓN CONTRACTUAL
- GESTIÓN FINANCIERA
- GESTIÓN LEGAL
- GESTIÓN DE BIENES Y SERVICIOS
- GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

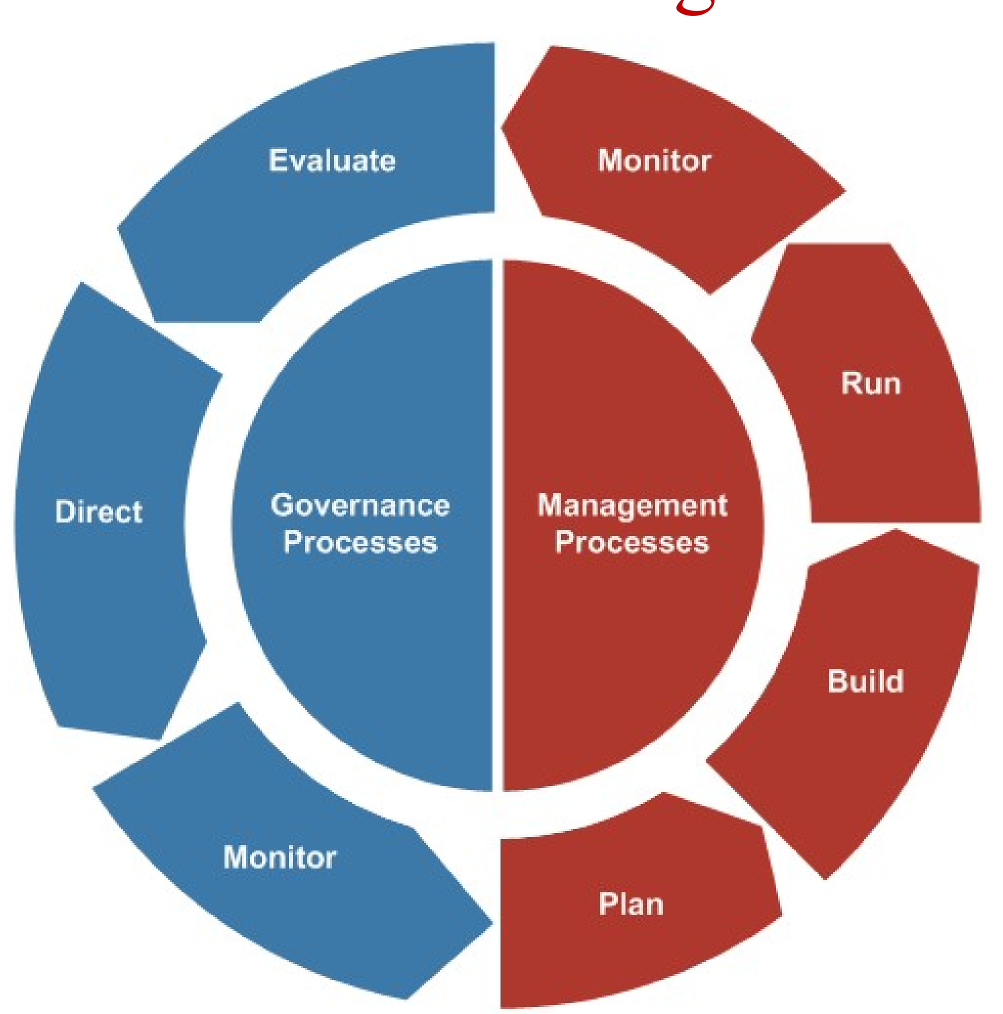
PROCESO DE EVALUACIÓN Y CONTROL

- MEJORA CONTINUA

REDUCCIÓN DE LA RESPONSABILIDAD PATRIMONIAL Y LA ACTIVIDAD LITIGIOSA



Procesos de Gobierno y Gerenciamiento de Tecnologia de Información (TI)



- ***Procesos de Gobierno***

Permite que las múltiples partes interesadas tengan una lectura organizada del análisis de opciones, identificación del norte a seguir y la supervisión del cumplimiento y avance de los planes establecidos,

- ***Procesos de Gestión***

Utilización prudente de medios (recursos, personas, procesos, practicas) para lograr un fin específico



Gobierno de TI en COBIT 5 (cont.)

Evaluar, Dirijir y Monitorear — **Procesos para el Gobierno Corporativo de TI**

- **EDM01** Asegurar que se fija el Marco de Gobierno y su Mantenimiento
- **EDM02** Asegurar la Entrega de Valor
- **EDM03** Asegurar la Optimización de los Riesgos
- **EDM04** Asegurar la Optimización de los Recursos
- **EDM05** Asegurar la Transparencia a las partes interesadas

Alinear, Planear y Organizar

- **APO01** Administrar el Marco de la Administración de TI
- **APO02** Administrar la Estrategia
- **APO03** Administrar la Arquitectura Corporativa
- **APO04** Administrar la Innovación
- **APO05** Administrar el Portafolio
- **APO06** Administrar el Presupuesto y los Costos
- **APO07** Administrar el Recurso Humano
- **APO08** Administrar las Relaciones
- **APO09** Administrar los Contratos de Servicios
- **APO10** Administrar los Proveedores
- **APO11** Administrar la Calidad
- **APO12** Administrar los Riesgos
- **APO13** Administrar la Seguridad

Construir, Adquirir e Implementar

- **BAI01** Administrar Programas y Proyectos
- **BAI02** Administrar la Definición de Requerimientos
- **BAI03** Administrar la Identificación y Construcción de Soluciones
- **BAI04** Administrar la Disponibilidad y Capacidad
- **BAI05** Administrar la Habilitación del Cambio
- **BAI06** Administrar Cambios
- **BAI07** Administrar la Aceptación de Cambios y Transiciones
- **BAI08** Administrar el Conocimiento
- **BAI09** Administrar los Activos
- **BAI10** Admnistrar la Configuración

Entregar, Servir y Dar Soporte

- **DSS01** Administrar las Operaciones
- **DSS02** Administrar las Solicitudes de Servicios y los Incidentes
- **DSS03** Administrar Problemas
- **DSS04** Administrar la Continuidad
- **DSS05** Administrar los Servicios de Seguridad
- **DSS06** Administrar los Controles en los Procesos de Negocio

Monitorear, Evaluar y Valorar

- **MEA01** Monitorear, Evaluar y Valorar el Desempeño y Cumplimiento
- **MEA02** Monitorear, Evaluar y Valorar el Sistema de Control Interno
- **MEA03** Monitorear, Evaluar y Valorar el Cumplimiento con Requisitos Externos

Procesos para la Administración de TI Corporativa



AUDIRISK

Planeación Anual de la Auditoría Interna "Basada en Riesgos"

Ejemplo de Universo Auditable

COMPONENTES	CANTIDAD
1. Procesos del Modelo de operación (Mapa de Procesos).	40
2. Aplicaciones de Computador	20
3. Procesos de Soporte de Servicios de TIC.	12
4. Procesos de Suministro de Servicios de TIC	12
TOTAL COMPONENTES	**84**



Identificar el Universo de Riesgos Aplicable a la Empresa

"Un conjunto finito y global de CATEGORIAS O CLASES DE RIESGO que pudieran presentarse en las operaciones de negocio (procesos estratégicos, misionales y de soporte) de la Organización" .

Ejemplos de Categorías o Clases de Riesgo:

- Fraude Interno.
- Sanciones Legales.
- Pérdida de Imagen o de Reputación.
- Estratégico





Identificar el Universo de Riesgos Aplicable a la Empresa

Qué es una Categoría o Clase de Riesgo ?.

“Son nombres genéricos utilizados para clasificar y agrupar los ***eventos de riesgo negativos o amenazas*** que podrían causar daños a los activos de la empresa y obstaculizar la consecución de los objetivos de la organización.

Por ejemplo, para el SARO se establecen siete (7) categorías de riesgo; para SARLAFT 4 categorías y para MECI cinco (5) categorías.

Categorías de Riesgo a Considerar en el Universo de Riesgos de las Organizaciones

Clases de Eventos de Riesgo Operativo
Modelo SARO
(CE 041 de 2007, SFC)

1. Fraude Interno.
2. Fraude Externo.
3. Fallas en la Atención a los Clientes.
4. Daños a Activos Físicos.
5. Fallas en Relaciones Laborales.
6. Fallas Tecnológicas.
7. Errores en Administración y Ejecución de Procesos.

Clases de Riesgos De LA / FT - Modelo SARLAFT
(CE 013 de 2013, SFC)

1. Riesgo Reputacional.
2. Riesgo Legal.
3. Riesgo Operativo.
4. Riesgo de Contagio



Categorías de Riesgo a Considerar en el Universo de Riesgos de las Organizaciones

Clases de Riesgo Modelo MECI:

1. Estratégico
2. Operativo
3. Financiero.
4. De cumplimiento.
5. De Tecnología.
6. De Corrupción

Clases de Riesgo Modelo AUDIRISK

1. Hurto / Fraude.
2. Sanciones Legales
3. Pérdida de Credibilidad Pública
4. Desventaja Competitiva.
5. Costos Excesivos
6. Pérdida de Ingresos.
7. Daño / Destrucción de Activos
8. Decisiones Erróneas



Categorías de Riesgo a Considerar en el Universo de Riesgos de las Organizaciones

Riesgos en el Sector Salud - Res 1740 de 2008 MPS

Administración de Riesgos de Salud:

1. De concentración de riesgos y hechos catastróficos.
2 De incrementos inesperados en los índices de Morbilidad y de costos de atención.
3. De cambios permanentes en las condiciones de salud o cambios tecnológicos.
4. De Insuficiencia de reservas técnicas.
5. De comportamiento.

Administración de Riesgo Operativo

- Riesgo Operativo
- Riesgo Legal y Regulatorio.
- Riesgo Reputacional



Categorías de Riesgo a Considerar en el Universo de Riesgos de las Organizaciones

Riesgos en el Sector Salud - Res 1740 de 2008 MPS

Administración de Riesgos Generales del Negocio

1. Riesgo Estratégico.
2. Riesgo de Crédito.
3. Riesgo de Mercado.
4. Riesgo de Liquidez.

Otros Requerimientos

- Planes de continuidad del negocio.
- Registro de Eventos de Riesgo Ocurridos





Categorías de Riesgo a Considerar en el Universo de Riesgos de las Organizaciones

Clasificación de los Riesgos Financieros

- Riesgo de Mercado.
- Riesgo de Crédito.
- Riesgo de Liquidez.
- Riesgo Legal.
- Riesgo Operativo.
- Riesgo de Reputación.



Planeación Anual de la Auditoría Interna "Basada en Riesgos"

Uso del Universo de Riesgos de la Empresa en la Planeación de la Auditoría

Universo de Categorías ó Clases de Riesgo

Aplicables a la empresa

Aplicables al Componente objeto de Auditoría

"Críticas para el Componente" (3 ó 4)

SARM
SARO
SARLAFT
Otras

Pueden presentarse en el componente.

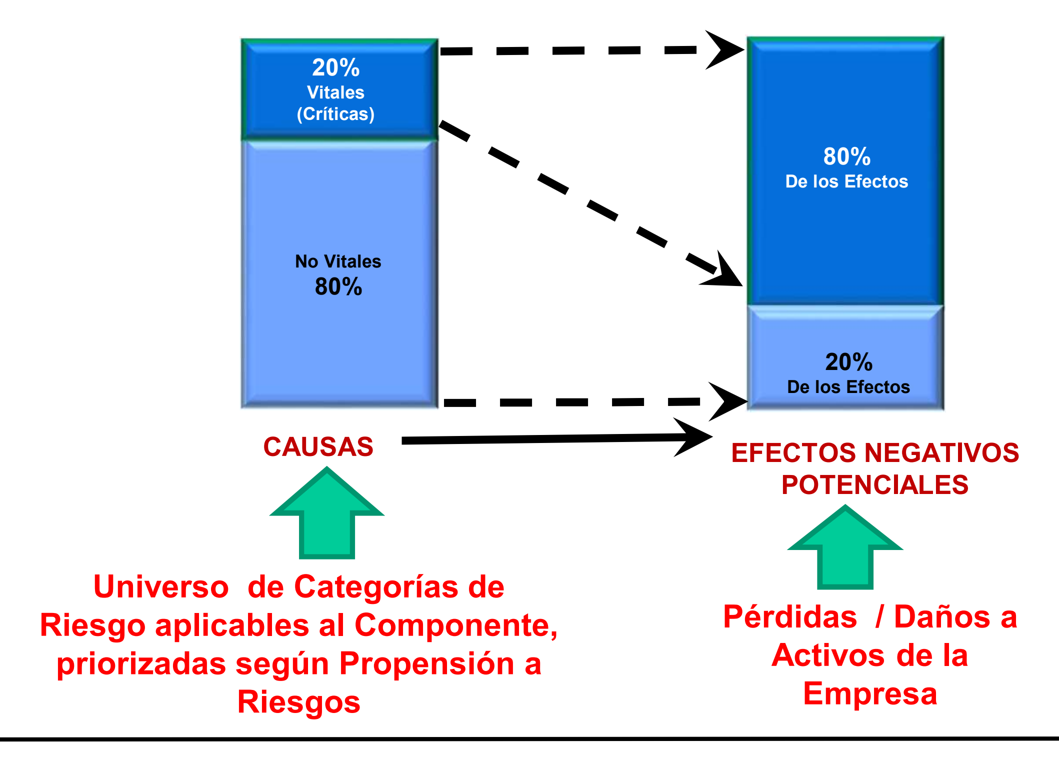
Para enfatizar en la Planeación y ejecución de la Auditoría con enfoque "Basada en Riesgos Críticos".



Planeación Anual de la Auditoría Interna "Basada en Riesgos"

Auditoría a los Componentes del Plan Anual

Aplicación Principio de Pareto / Regla 80:20







Planeación Anual de la Auditoría Interna "Basada en Riesgos"

Articulación del Plan Anual con el proceso de Auditoría Basada en Riesgos.

Planeación Anual Basada en Riesgos.

- ❑ Auditorias a realizar en el año.
- ❑ Categorías de riesgo críticas por componente.

Proceso de Auditoría "Basada en Riesgos Críticos"

Planeación detallada y Familiarización

- ❖ Memorando de planeación.
- ❖ Actualización de archivo permanente

Identificación y Análisis Riesgos Inherentes.

Eventos/Amenazas que pueden presentarse (20-30)

- E: Extremo
- A: Alto
- M: Moderado
- B: Bajo

Cubo de riesgos

Ejecución Auditoría

- ❖ Evaluación control Interno.
- ❖ Pruebas de Cumplimiento
- ❖ Pruebas sustantivas.

Informes con Resultados de la Auditoría.

- ❖ Evaluación control Interno.
- ❖ Pruebas de Cumplimiento
- ❖ Pruebas sustantivas.

Seguimiento a hallazgos de Auditoría

- ❖ Evaluación control Interno.
- ❖ Pruebas de Cumplimiento
- ❖ Pruebas sustantivas.



Elaboración del Plan Anual de Auditoría Interna, Basado en Riesgos".

Pasos de la Metodología.

3. **Estimar (medir) la Propensión (Exposición) a Riesgos de los Componentes del** ***Universo de Auditoría.***

   - **Elaborar TRES (3) cuestionarios con Factores de Riesgo (preguntas) y Opciones de respuesta**: a) Procesos del Modelo de Operación; b) Aplicaciones de Computador o módulos de ERPs y c) los procesos de Soporte y Prestación de Servicios de Sistemas (TIC). - Formato 2

   - **Estimar Impacto de las Categorías de Riesgo sobre los Factores de Riesgo (preguntas de los Cuestionarios – Formato 3)**



AUDIRISK

Elaboración del Plan Anual de Auditoría Interna, Basado en Riesgos".

Pasos de la Metodología.

3. **Estimar (medir) la Propensión (Exposición) a Riesgos de los Componentes del *Universo de Auditoría.***

   - **Responder Cuestionarios y procesar las Respuestas. Estimar la exposición (propensión) a riesgos de cada proceso o sistema**: Un puntaje entre 0 y 100 (También se conoce como "Nivel de Seguridad Requerida").

   - **Priorizar Componentes del Universo de Auditoría, según Exposición a Riesgos.** Clasificar de mayor a menor puntaje, los procesos y sistemas del Universo de Auditoría, según su puntaje de Exposición (propensión a Riesgos).



AUDIRISK

Elaboración del Plan Anual de Auditoría Interna, Basado en Riesgos”.

Prioridades de los componentes del Universo de Auditoría para el Plan Anual según su propensión (Exposición) a Riesgos.

Puntaje de propensión (Exposición) a Riesgos.	Prioridad	Observaciones
Mayor que 80	**1**	Debe incluirse en el plan Anual.
Entre 60 y 80	**2**	Después de componentes prioridad 1
Entre 40 y 60	**3**	Después de componentes prioridad 2
Entre 20 y 40	**4**	No incluir en el plan
Menor de 20	**5**	No incluir en el plan.



Elaboración del Plan Anual de Auditoría Interna, Basado en Riesgos".

Pasos de la Metodología.

3. **Estimar (medir) la Propensión a Riesgos de los Componentes del** ***Universo de Auditoría. – Ejemplo de cuestionario para procesos del Modelo de Operación.***

Factor de Riesgo 1: Convertibilidad a dinero efectivo, de los recursos y activos que se manejan en el proceso (Títulos Valores, Información y secreto profesional entre otros).

No	Criterios de evaluación	Peso
a)	De Difícil convertibilidad	10
b)	Moderada dificultad para convertirlos en dinero efectivo	60
c	Fácilmente convertibles a dinero efectivo	100



Elaboración del Plan Anual de Auditoría Interna, Basado en Riesgos".

Pasos de la Metodología.

3. Estimar (medir) la Propensión a Riesgos de los Componentes del *Universo de Auditoría. – Ejemplo de cuestionario para procesos del Modelo de Operación.*

Factor de Riesgo 2: Dependencia de las operaciones del proceso con respecto a la Tecnología de Información

No	Criterios de evaluación	Peso
a)	La realización de las operaciones NO DEPENDE del funcionamiento de los sistemas de TIC. Las operaciones se realizan sin ayuda de los sistemas de TIC.	10
b)	La realización de las operaciones DEPENDE PARCIALMENTE del funcionamiento de los sistemas de TIC. Sin sistemas las operaciones no pueden realizarse	60
c)	La realización de las operaciones DEPENDE SIGNIFICATIVAMENTE del funcionamiento de los sistemas de TIC. Sin sistemas las operaciones no pueden realizarse.	100



Elaboración del Plan Anual de Auditoría Interna, Basado en Riesgos".

Pasos de la Metodología.

3. **Estimar (medir) la Propensión a Riesgos de los Componentes del *Universo de Auditoría. – Ejemplo de cuestionario para procesos del Modelo de Operación.***

Factor de Riesgo 3: Cantidad de puntos de operación o de servicio que originan transacciones (información) para las operaciones del proceso.

No	Criterios de evaluación	Peso
a)	Menos de cinco (5)	30
b)	Entre 6 y 10	60
c)	Entre 11 y 50	90
d)	Más de 50	100



AUDIRISK

Cuestionario para Estimar Exposición (Propensión) a Riesgos

CUESTIONARIO PARA MEDIR (ESTIMAR) LA PROPENSION A RIESGOS DE LOS PROCESOS DEL MODELO DE OPERACIÓN DE LA EMPRESA		
FORMATO No. 1		
Proceso: ____		
Factores de Riesgo para Procesos del Mapa de Procesos / Cadena de Valor	Peso Respuesta	Ponderac. factor
1. Contribución al logro de los objetivos institucionales		10
a) Es un proceso de supervisión y control	40	
b) Es un proceso de Apoyo	50	
c) Es un proceso Misional	90	
d) Es un proceso Estratégico	70	
2. Tiempo Máximo de Interrupción Permisible (Tiempo de tolerancia a Fallas) de las operaciones del proceso sin que la Entidad sufra impacto signficativo		15
a) Menos de 8 horas	100	
b) Entre 8 y 16 horas	80	
c) Entre 16 y 32 horas	50	
d) Mas de 32 hora	20	
3. Valor de las pérdidas o costos excesivos como consecuencia de las interrupciones de las operaciones (proceso) superiores a dos días		10
a) Menores a 10 millones	20	
b) Entre 10 y 15 millones	50	
c) Entre 15 y 20 millones	80	
d) Mas de 20 millones	90	
4. Dependencia del proceso respecto al funcionamiento de los sistemas de informacion automatizados para el manejo de las operaciones		15
a) El proceso depende completamente de los sistemas de informacion	90	
b) Mas del 50% de las operaciones del proceso dependen de los sistemas	70	
c) Entre el 30 y 50% de las operaciones del proceso dependen de los sistemas	50	
d) Menos del 30 % de las operaciones del proceso dependen de los sistemas	20	
e) El proceso no depende para nada de los sistemas de informacion	0	
5. Importancia de la información que maneja y/ o genera (*)		15
a) Vital para la continuidad de negocios de la organización	25	
b) De valor Estratégico	25	
c) De valor confidencial para la organización	25	
d) De valor para la toma de decisiones	25	



AUDIRISK

Establecer Impacto de las Categorías de Riesgo sobre los Factores de Riesgo

Asignación de Pesos al Impacto de los Factores de Riesgo sobre Clases de Riesgo - Formato No. 3

Proceso: ______________________________

No	Factores de Riesgo para Procesos del Mapa de Procesos / Cadena de Valor	Ponderac. factor	Exposicion a Riesgos %								Totales
			Fraude	sanciones Legales	Perdida de Activos	Costos Excesivos	Perdida de Ingresos	Desventaja competitiva	Perdida de Reputacion	Decisiones erróneas	
1	Contribución al logro de los objetivos institucionales	10							80	20	100,00
2	Tiempo Máximo de Interrupción Permisible (Tiempo de tolerancia a Fallas) de las operaciones del proceso sin que la Entidad sufra impacto signficativo	15	15	10		35			20	20	100,00
3	Valor de las pérdidas o costos excesivos como consecuencia de las interrupciones de las operaciones (proceso) superiores a dos días	10	10	10	10	30			30	10	100,00
4	Dependencia del proceso respecto al funcionamiento de los sistemas de información automatizados para el manejo de las operaciones	15	10	10	10	20	10	20	10	10	100,00
5	Importancia de la información que maneja y/ o genera	15	15	10		25	10	15	10	15	100,00
6	Participación en el presupuesto de gastos anuales generados por la entidad	15	20	10	10	10	10	10	10	20	100,00



AUDIRISK

Medición de la Propensión (Exposición) a Riesgos por componente

ELABORACION PLAN ANUAL DE AUDITORIA DE SISTEMAS.

Formato para Medir Impacto de las Clases de Riesgo en los Proceso de TI (Formato 4).

Proceso de TI: ____________________________

Factores de Riesgo Evaluados	Estimación del Impacto de los Riesgos en el Proceso (peso del Factor * Ponderación del Impacto del Factor en las Clases de Riesgo)							Suma Puntajes Exposición a Riesgos del Factor
	Fraude Interno	Fraude Externo	Conflictos con Clientes	Conflictos Laborales	Problemas de proceso	Daño Activos Físicos	Fallas Tecnológicas	
1. Nivel de desempeño o funcionamiento actual del proceso de TI (*)								
2. Antecedentes de calificación del desempeñodel proceso de TI) (*)								
Suma Puntajes de Exposición al Riesgo por riesgo	NNNN							NNNN
Ponderación %								100%
Ranking del riesgo para el proceso de TI								

(*) Por cada riesgo se coloca el valor que resulta de multiplicar el peso del Factor * Ponderación del Impacto del Factor en las Clases de Riesgo.



AUDIRISK

Propensión (Exposición) a Riesgos Estimada por componente

Estimar Exposición a Riesgos, por Clases de Riesgo y Factor de Riesgo en los Procesos del Modelo de Operación - Formato No. 4

Proceso: ___________________________________

No	Factores de Riesgo para Procesos del Mapa de Procesos / Cadena de Valor	Peso Respuesta (por factor de Riesgo)	Estimación del Impacto del Factor en las Categorías de Riesgos								Suma impactos-Expo. A riesgos Por factor	Ponderación Factores de Riesgo	Ranking Factores de Riesgo
			Fraude	sanciones Legales	Perdida de Activos	Costos Excesivos	Perdida de Ingresos	Desventaja competitiva	Perdida de Reputacion	Decisiones erróneas			
1	Contribución al logro de los objetivos institucionales	10	0	0	0	0	0	0	4	1	5	5,26	6
2	Tiempo Máximo de Interrupción Permisible (Tiempo de tolerancia a Fallas) de las operaciones del proceso sin que la Entidad sufra impacto signficativo	15	2,25	1,5	0	5,25	0	0	3	3	15	15,79	1
3	Valor de las pérdidas o costos excesivos como consecuencia de las interrupciones de las operaciones (proceso) superiores a dos días	10	1	1	1	3	0	0	3	1	10	10,53	2
4	Dependencia del proceso respecto al funcionamiento de los sistemas de información automatizados para el manejo de las operaciones	15	1,5	1,5	1,5	3	1,5	3	1,5	1,5	15	15,79	4
5	Importancia de la información que maneja y/ o genera	15	2,25	1,5	0	3,75	1,5	2,25	1,5	2,25	15	15,79	3
6	Participación en el presupuesto de gastos anuales generados por la entidad	15	3	1,5	1,5	1,5	1,5	1,5	1,5	3	15	15,79	5
7	Participación en el presupuesto de ingresos anuales generados por la Entidad	10	1	1	1	1	2	2	1	1	10	10,53	7
8	Participación en el presupuesto de Utilidades generadas para la Entidad	10	2	1	1	1	2	1	1	1	10	10,53	8
Exposicion a Riesgos por Categoria de Riesgo			13	9	6	18,5	8,5	9,75	16,5	13,75	95		
Ponderación de clases de riesgo			13,68	9,47	6,32	19,47	8,95	10,26	17,37	14,47			
Ranking Clases de Riesgo			4	6	8	1	7	5	2	3			



AUDIRISK

Matriz de Planeación de la Auditoria. Asignar Prioridades por riesgos y por procesos - Formato 5

Procesos de Tecnología de Información – COBIT	Suma Puntajes de Exposición al Riesgo por riesgo – (NNNN - formato 4)							Suma Puntajes Exposición a Riesgos del Proceso	Ranking del Proceso (prioridad)
	Fraude Interno	Fraude Externo	Conflictos con Clientes	Conflictos Laborales	Problemas de proceso	Daño Activos Físicos	Fallas Tecnológicas		
• AI1 : Identificar Soluciones Automatizadas									
• AI2 : Adquirir y Mantener Software de Aplicación									
• AI3 : Adquirir y Mantener Infraestructura de Tecnología									
• AI4: Habilitar la Operación y Uso									
• AI5: Obtener los Recursos de TI									
• AI6: Administración de Cambios									
• AI7: Instalar y Acreditar Soluciones y Cambios									
Ranking del riesgo para los procesos de TI en la Organización									





Matriz de Planeación Anual de la Auditoría Interna – Formato 5

Priorización de Componentes - Por Categoría de Riesgo y Propensión a Riesgos de los Componentes

No	Procesos	Puntajes de Exposición al Riesgo por clase de Riesgo – Tomados de formato 4								Exposición a Riesgos - Proceso	Pondera-ción del proceso	Ranking Proceso
		Fraude	sanciones Legales	Perdida de Activos	Costos Excesivos	Perdida de Ingresos	Desventaja competitiva	Perdida de Reputacion	Decisiones erróneas			
1	Planeación Estrategica Corporativa	1,775	1,25	0,2	3,525	0,75	1,125	7,55	3,325	19,5	4%	8
2	Gestion de cambios	4,125	3,1	2,05	7,025	2,8	3,725	8,4	4,775	36	8%	6
3	CDPs	3,3375	2,775	1,65	6,9625	1,925	3,4625	11,125	5,5125	36,75	8%	7
4	Cuentas Corrientes	10,5875	7,575	4,95	16	6,675	8,0875	18,08	12,6375	84,755	18%	2
5	Ahorros	10,9375	7,675	5,35	15,5125	7,475	8,4875	17,88	12,4375	85,76	19%	1
6	Inversiones	7,475	5,3	3,35	12	4,2	5,625	14,7	9,575	62	13%	4
7	TaRJETAS DE Credito	9,15	6,45	3,45	15,60	4,95	6,15	16,95	10,8	73,5	16%	3
8	Gestion de talento humano	1,762	1,12	15,35	6,53	1,293	12,32	5,232	18,2	61,807	13%	5
	TOTALES POR CATEGORIA DE RIESGO	49,1495	35,245	36,35	83,0925	30,068	48,9825	99,917	77,2625	460,067		
	Ponderación Categorías de Riesgo	11%	8%	8%	18%	7%	11%	22%	17%			
	Ranking de las Categorías de Riesgo	5	7	6	2	8	4	1	3			



Elaboración del Plan Anual de Auditoría Interna, Basado en Riesgos".

Pasos de la Metodología:

4. Generar *PANORAMAS DE RIESGO* para cada uno de los componentes del universo de auditoría:

- Propensión de cada proceso ó sistema, a *las categorías de riesgo del Universo de Riesgos de la Empresa.*
- Categorías de Riesgo Críticas en cada proceso del Modelo de Operación.
- Categorías de Riesgo Críticas en cada proceso de TI.
- Categorías de Riesgo Críticas en cada Aplicación de Computador.



Generación de Panoramas de Riesgo por Componentes del Universo de Auditoría

Ejemplo de Perfiles por Categorías de Riesgo en los Procesos del Modelo de Operación

Categoría de Riesgo: **Fraude Interno**

Procesos del Modelo de Operación de la Empresa	% Exposición a Riesgos	Ranking (prioridad)
Gestión del Talento Humano	65%	4
Gestión de Compras.	80%	3
Gestión de Inventarios	92%	1
Gestión de Producción	85%	2





Generación de Panoramas de Riesgo por Componentes del Universo de Auditoría

Ejemplo de Priorización de las Categorías de Riesgo en los Procesos del Modelo de Operación

Procesos del Modelo de Operación de la Empresa	% Exposición a Riesgos	Ranking (Prioridad)
Gestión Talento Humano	78%	3
Gestión de Compras.	62%	5
Gestión de Inventarios.	84%	2
Gestión de Producción	90%	1
Gestión de Proveedores	63%	4





Elaboración del Plan Anual de Auditoría Interna, Basado en Riesgos”.

Pasos de la Metodología:

5. Seleccionar los componentes del Universo de Auditoría, que serán auditados en el año, *según porcentaje de exposición a riesgos - Con base en la Matriz de Planeación Anual* . Formato 5



Matriz de Planeación Anual de la Auditoría Interna – Formato 5

Priorización de Componentes - Por Categoría de Riesgo y Propensión a Riesgos de los Componentes

No	Procesos	Puntajes de Exposición al Riesgo por clase de Riesgo – Tomados de formato 4								Exposición a Riesgos - Proceso	Pondera-ción del proceso	Ranking Proceso
		Fraude	sanciones Legales	Perdida de Activos	Costos Excesivos	Perdida de Ingresos	Desventaja competitiva	Perdida de Reputacion	Decisiones erróneas			
1	Planeación Estrategica Corporativa	1,775	1,25	0,2	3,525	0,75	1,125	7,55	3,325	19,5	4%	8
2	Gestion de cambios	4,125	3,1	2,05	7,025	2,8	3,725	8,4	4,775	36	8%	6
3	CDPs	3,3375	2,775	1,65	6,9625	1,925	3,4625	11,125	5,5125	36,75	8%	7
4	Cuentas Corrientes	10,5875	7,575	4,95	16	6,675	8,0875	18,08	12,6375	84,755	18%	2
5	Ahorros	10,9375	7,675	5,35	15,5125	7,475	8,4875	17,88	12,4375	85,76	19%	1
6	Inversiones	7,475	5,3	3,35	12	4,2	5,625	14,7	9,575	62	13%	4
7	TaRJETAS DE Credito	9,15	6,45	3,45	15,60	4,95	6,15	16,95	10,8	73,5	16%	3
8	Gestion de talento humano	1,762	1,12	15,35	6,53	1,293	12,32	5,232	18,2	61,807	13%	5
	TOTALES POR CATEGORIA DE RIESGO	49,1495	35,245	36,35	83,0925	30,068	48,9825	99,917	77,2625	460,067		
	Ponderación Categorías de Riesgo	11%	8%	8%	18%	7%	11%	22%	17%			
	Ranking de las Categorías de Riesgo	5	7	6	2	8	4	1	3			



Elaboración del Plan Anual de Auditoría Interna, Basado en Riesgos".

Pasos de la Metodología.

6. **Definir Trabajos de Auditoría a realizar durante el Año, por cada Componente seleccionado para el Plan Anual de Auditoría. Una o más de las siguientes alternativas de Auditoría:**

   1) Auditorías a un proceso o sistema, hasta la Evaluación del Control Interno.

   2) Pruebas de Auditoria (de Cumplimiento y Sustantivas) – A un (1) Proceso en Múltiples Sitios de Prueba (una muestra de áreas ó terceros que intervienen en las operaciones).

   3) Pruebas de Auditoría (de cumplimiento y Sustantivas) a Múltiples Procesos en un Area de Operación (Sitio de Prueba).

Elaboración del Plan Anual de Auditoría Interna, Basado en Riesgos".

Pasos de la Metodología.

7. Definir objetivo, alcance y recursos requeridos para las auditorías basadas en riesgos, incluidas en el Plan Anual.

a) Objetivo general.

b) Alcance - Actividades y categorías de riesgo que revisará

c) Personal asignado: Con personal de planta u Outsourcing

d) Duración estimada en horas.

e) Fecha de iniciación y finalización.



Elaboración del Plan Anual de Auditoría Interna, Basado en Riesgos".

Pasos de la Metodología.

8. Presentar Alternativas para ejecutar Plan Anual de Auditoría y obtener los recursos requeridos (integra todos los componentes seleccionados para el plan Anual de Auditoría).

a) Definir trabajos a Contratar con Terceros o a realizar con Mezcla de personal de planta y terceros.

b) Definir Otros recursos requeridos (financieros y tecnológicos)

c) Elaborar Cronograma general y grafico de barras.



Elaboración del Plan Anual de Auditoría Interna, Basado en Riesgos”.

Pasos de la Metodología:

9. Generar el Plan Anual de Auditoría, *Basado en la Valoración de la Propensión a Riesgos*, que será presentado a consideración y aprobación del Comité de Auditoría y la Dirección de la Empresa.

10. Presentar y sustentar el Plan Anual de Auditoría.





Módulo 4

Desarrollo de Auditorías Basadas en Riesgos Críticos, a procesos y sistemas de información





Módulo 4: Desarrollo de Auditorías Basadas en Riesgos

Objetivos:

Para una muestra de riesgos inherentes (por ejemplo, 30 eventos), el software AUDIRISK:

1. ***Conduce*** el desarrollo de las fases, etapas y pasos del proceso de auditoría a los procesos del modelo de operación de la empresa, los procesos de la infraestructura de TI y las Aplicaciones de Computador.
   - Planeación Basada en Riesgos.
   - Evaluación del Control Interno.
   - Pruebas de Cumplimiento.
   - Pruebas Sustantivas.
   - Generar los Informes con los resultados de la Auditoría – 4 informes.
   - Seguimiento a hallazgos de la auditoría.

2. Elaborar los papeles de trabajo de la auditoría – formato electrónico.

3. Controlar el tiempo asignado para el desarrollo de cada auditoría.





Desarrollo de Auditorías Basadas en Riesgos

Auditoria Basada en Riesgos

Requerimiento del negocio y de seguridad

Por cada Proceso ó Sistema

1. Planeación basada en riesgos
2. Ejecución
   - •Evaluar Controles Establ.
   - •Pruebas de cumplimiento
   - •Pruebas sustantivas
3. Comunicación de resultados
4. Seguimiento

✓ Dictamen satisfacción requerimientos del negocio y de seguridad





Módulo 4: Desarrollo de Auditorías Basadas en Riesgos

Concepto de "Auditoría Basada en Riesgos"

- La **auditoría** es el examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado.

- La **Auditoría Basada en Riesgos** *es una forma de conducir auditorías internas o externas de diferentes tipos (operativa, de estados financieros, de sistemas de información, de sistemas de gestión),* ***con enfoque proactivo y preventivo****, basando su planeación y desarrollo en la revisión de* ***una muestra de eventos de riesgo negativos,*** *que pudieran generar daños o pérdidas significativas de activos los procesos o sistemas y la actividad económica de una organización, para confirmar si los procedimientos, controles y la información se ajustan a lo fijado por las leyes, las reglas del negocio y las buenas y mejores prácticas de control interno y seguridad.*





Módulo 4: Desarrollo de Auditorías Basadas en Riesgos

El Enfoque Proactivo / Preventivo de la Auditoría Basada en Riesgos

- El objetivo principal de la Auditoría **NO ES**: *"Detectar los errores e irregularidades que podrían presentarse en la operación de los procesos y sistemas de la organización* ***- No es detectar o descubrir eventos de riesgo ocurridos".***

- El objetivo de la Auditoría PROACTIVA - PREVENTIVA es *evaluar y verificar que los procesos y sistemas de la empresa funcionan de manera eficaz, eficiente y segura y están protegidos adecuadamente contra los riesgos críticos que pudieran presentarse en las operaciones.* ***Anticiparse a la ocurrencia de los eventos de riesgos para ayudar a prevenirlos*****.**

- El tiempo de la Auditoría es menor o igual que el tiempo de los eventos de riesgo.





Módulo 4: Desarrollo de Auditorías Basadas en Riesgos

Considera dos (2) Estados de los Riesgos para una Muestra de Riesgos Inherentes seleccionados por la Auditoría.

- **Riesgos Inherentes:** ***Eventos negativos*** **(amenazas) que pueden presentarse** en las actividades y servicios del proceso o sistema y obstruir la consecución de los objetivos estratégicos y de las operaciones de negocio de la Organización. En la estimación de su SEVERIDAD no se tienen en cuenta los controles establecidos.

  Punto de partida de la Auditoría: Verificar que la empresa está protegida adecuadamente para **una muestra** de riesgos inherentes que podrían presentarse.

- **Riesgo Residual:** Riesgo que permanece o persiste **después de Evaluación de Control Interno y Pruebas de Auditoría**, para la muestra de eventos negativos (amenazas) críticos seleccionados por la auditoría.

  Punto de llegada de la Auditoría: Determinar si el riesgo residual asumido por la empresa es **aceptable.**





Módulo 4: Desarrollo de Auditorías Basadas en Riesgos

Ejemplo:

Evento de Riesgo (Amenaza): **"Ingresar fecha que no corresponde a la lógica de las operaciones".**

Severidad Riesgo Inherente (Potencial): Riesgo antes de Controles y Pruebas de Auditoría.

Severidad: E - Extremo.

Acciones de Respuesta: Reducir (mitigar) el riesgo.

Controles:

- **Preventivos**: La fecha debe tener el formato dd/mm/aaaa; El día debe se menor o igual que 31; mes menor o igual que 12; año debe ser el actual.
- **Detectivos:** Validar que la fecha satisfaga los estándares – Los controles preventivos; Informar cuando no coinciden – "Error Fecha , Fecha No válida"; Disparar Alarma cuando se detecta una desviación respecto al "debería ser"; Bloquea – no deja continuar hasta que la fecha sea válida
- **Correctivos:** Debe volver a ingresar la fecha (Obliga); vuelve a validar los estándares y si no coinciden se emite mensaje, bloquea y exige que se ingrese nuevamente la fecha.

Severidad Riesgo Residual: Severidad del Riesgo no protegido o no cubierto por los controles verificados . **Severidad : B - Bajo** (Tolerable).





Etapas de la Auditoría "Basada en Riesgos Críticos"

FASE 1: PLANEACIÓN BASADA EN RIESGOS

1. **Pre- auditoría**
   - Memorando de Planeación
   - Programa de Trabajo

2. **Comprensión Proceso o Sistema**
   - Archivo Permanente
   - Caracterización

3. **Id. y Análisis de Riesgos**
   - Muestra de Riesgos Inherentes Críticos
   - Mapa de Riesgos Inherentes

4. **Contexto de Riesgos del proceso s. a Auditoría**
   - Cubo de Riesgos de la Auditoría



Etapas de la Auditoría "Basada en Riesgos Críticos"

FASES 2, 3 y 4: EJECUCION E INFORMES DE LA AUDITORIA

5

Evaluar Controles Establecidos

- Evaluar Diseño y Efectividad
- Medir / evaluar Riesgo Residual
- Informe – Evaluación Control Interno

6

Pruebas de Cumplimiento

- % Cumplim. Cont. y Proced. Claves
- Informes Pruebas de Cumplimiento

7

Pruebas Sustantivas

- A Exactitud Cifras Claves
- Informes Pruebas Sustantivas

8

Seguimiento Hallazgos Informes de Auditoría

- Informe Estado Acciones de Mejora





Auditoría Proactiva Basada en Riesgos

Análisis de los 6 Elementos del Riesgo (*)

Por cada Riesgo Inherente Negativo



(*) Evento de Riesgo Negativo, según ISO 31000





Módulo 4: Desarrollo de Auditorías Basadas en Riesgos

El enfoque Proactivo / Preventivo de la Auditoría Basada en Riesgos

Por cada **riesgo inherente (amenaza) de la "muestra de riesgos seleccionada por la Auditoría",** (Máximo 30, Mínimo 18), el análisis de la auditoría enfatiza al menos en siete (7) elementos del riesgo:

1. Activos impactados – Tangibles e intangibles.
2. Vulnerabilidades que crean el ambiente propicio para que las amenazas se materialicen.
3. Agentes generadores y factores de riesgo: personas y actos de la naturaleza.
4. Severidad o Nivel Exposición al riesgo (Combina frecuencia estimada de ocurrencia anual e impacto financiero y operacional).
5. Consecuencias que tendría que afrontar la organización en caso de ocurrir.
6. Fuentes del riesgo (actividades del proceso y áreas organizacionales o terceros).
7. Los controles establecidos para gestionar el riesgo.





Mapa de Riesgos Inherentes

De la Muestra de Riesgos Seleccionada parea la Auditoría

PROBABILIDAD		1 Insignificante	2 Menor	3 Moderado	4 Mayor	5 Catastrófico
Casi Cierto	5	A	A	E	E	E
Probable	4	M	A	A	E	E
Posible	3	B	M	A	E	E
Poco probable	2	B	B	M	A	E
Raro	1	B	B	M	A	A

IMPACTO EN LA ORGANIZACION

E	Extremo
A	Alto
M	Moderado
B	Bajo





Auditoría Basada en Riesgos Críticos

Escala para evaluar Severidad de los Riesgos

Niveles de Severidad del Riesgo (Inherente o Residual)	Consecuencias en caso de Presentarse
1 ó B: Bajo	La ocurrencia del evento (amenaza) tendría consecuencias leves, tolerables por la organización. Se puede gestionar mediante procedimiento de rutina. En caso de presentarse no desestabiliza a la organización.
2 ó M: Moderado	En caso de presentarse ocasionaría consecuencias que superan el nivel de tolerancia de la organización. Requiere atención de la Gerencia. Debe ser gestionado con controles para disminuir su impacto o la frecuencia de ocurrencia.
3 ó A: Alto	En caso de presentarse ocasionaría consecuencias financieras y operacionales de impacto severo o significativo para la organización. Es necesaria la atención inmediata de la Gerencia. Debe gestionarse con acciones para transferir el riesgo a terceros, dispersar el riesgo y reducir su impacto o la frecuencia de ocurrencia.
4ó E: Extremo	Su ocurrencia ocasionaría consecuencias financieras y operacionales de impacto catastrófico para la organización. Es necesaria la atención inmediata de la Gerencia. Debe gestionarse con mecanismos para **evitar su ocurrencia o** transferir el riesgo a terceros, dispersar el riesgo y reducir su impacto o la frecuencia de ocurrencia.





Módulo 4: Desarrollo de Auditorías Basadas en Riesgos

Evaluación del Diseño de los Controles – Protección Existente . Por evento de riesgo.

Aplica dos (2) criterios para "Evaluar Diseño de los Controles establecidos, por cada evento de riesgo inherente (amenaza).

- **Se eliminan las Vulnerabilidades identificadas en el Análisis del Riesgo?**
  - ✓ Ninguna.
  - ✓ Algunos
  - ✓ Todas.
- **Se Neutraliza o bloquea a todos los Agentes Generadores del Riesgo identificados en el Análisis de Riesgos.**
  - ✓ Ninguno.
  - ✓ Algunos
  - ✓ A Todos.





Módulo 4: Desarrollo de Auditorías Basadas en Riesgos

Evaluación de Efectividad Individual de los Controles por Riesgo Inherente.

Aplica doce (12) criterios parametrizables para "Evaluar la Efectividad Individual de los Controles establecidos, por cada evento de riesgo inherente (amenaza).

Estratos de Pareto	Rangos de Puntaje Obtenido Desde – hasta	Efectividad Individual
1	Mayor que 48	5: Muy Alta
2	Mayor que 36 y menor que 48	4: Alta
3	Mayor que 24 y menor que 36	3: Moderada
4	Mayor que 12 y menor que 24	2: Baja
5	Mayor que 0 y menor que 12	1: Muy Baja





Módulo 4: Desarrollo de Auditorías Basadas en Riesgos

Evaluación de la Efectividad Colectiva de los Controles por Riesgo Inherente.

Aplica dos alternativas de tres (3) criterios para "Evaluar la Efectividad (eficacia + eficiencia)" de los Controles establecidos, por cada evento de riesgo inherente (amenaza**).**

- **Para la Eficacia de los Controles**
  - ✓ Se utiliza Enfoque de los **3 niveles o anillos de Seguridad o Líneas de Defensa ? – Al menos 3 controles que hagan SINERGIA. Criterio Obligatorio.**
  - ✓ El promedio de la Efectividad Individual de los Controles es Mayor que 4.0
- **Para la Eficiencia de los Controles.** El Costo / Beneficio es RAZONABLE (Los controles reducen en porcentaje significativo la Pérdida ´Anual Estimada).

AUDIRISK

Evaluación Efectividad de los Controles, Por Evento de Riesgo

BC AUDITORÍA
Buenas y Mejores Prácticas de Controles

Ⓓ

BC AUDITORÍA
Muestra de Eventos de Riesgo Inherente

Seleccionar Evento

Definir Controles Aplicables

Identificar Controles Existentes

Ⓐ

Ⓐ

Satisfacen Criterio " 3 Anillos de Seguridad"

NO

Satisfacen los otros 2 Criterios

NO

Satisfacen 1 Criterio

NO

Controles Son: "1: Muy Deficientes"

Ⓑ

SI

SI

SI

Controles Son: "3 -Insuficientes"

Controles Son: "2::Deficientes"

Ⓑ

Controles son : "5: Apropiados"

SI

Satisfacen Otro Criterio

NO

Ⓒ

Controles Son: "4: Mejorables"

Ⓑ

Ⓑ

Generar Hallazgo de Auditoría

Analizar Hallazgo

Ⓒ

Hay Más Eventos

NO

Generar Reportes de Evaluación de Controles

Generar Informe de Auditoría

SI

Ⓓ

Finalizar





Enfoque de las Tres Anillos Seguridad o Líneas de Defensa

EVENTOS DE RIESGO INHERENTE (Amenazas)

A1 → A2 → A3 →

BARRERA PREVENTIVA

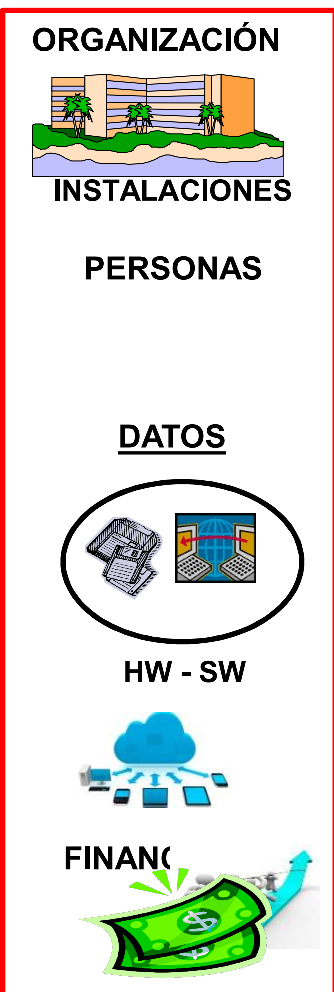
A2 → A3 →

BARRERA DETECTIVA

A3 →

BARRERA CORRECTIVA

FEEDBACK







Etapa 5: Evaluación del Control Interno Existente

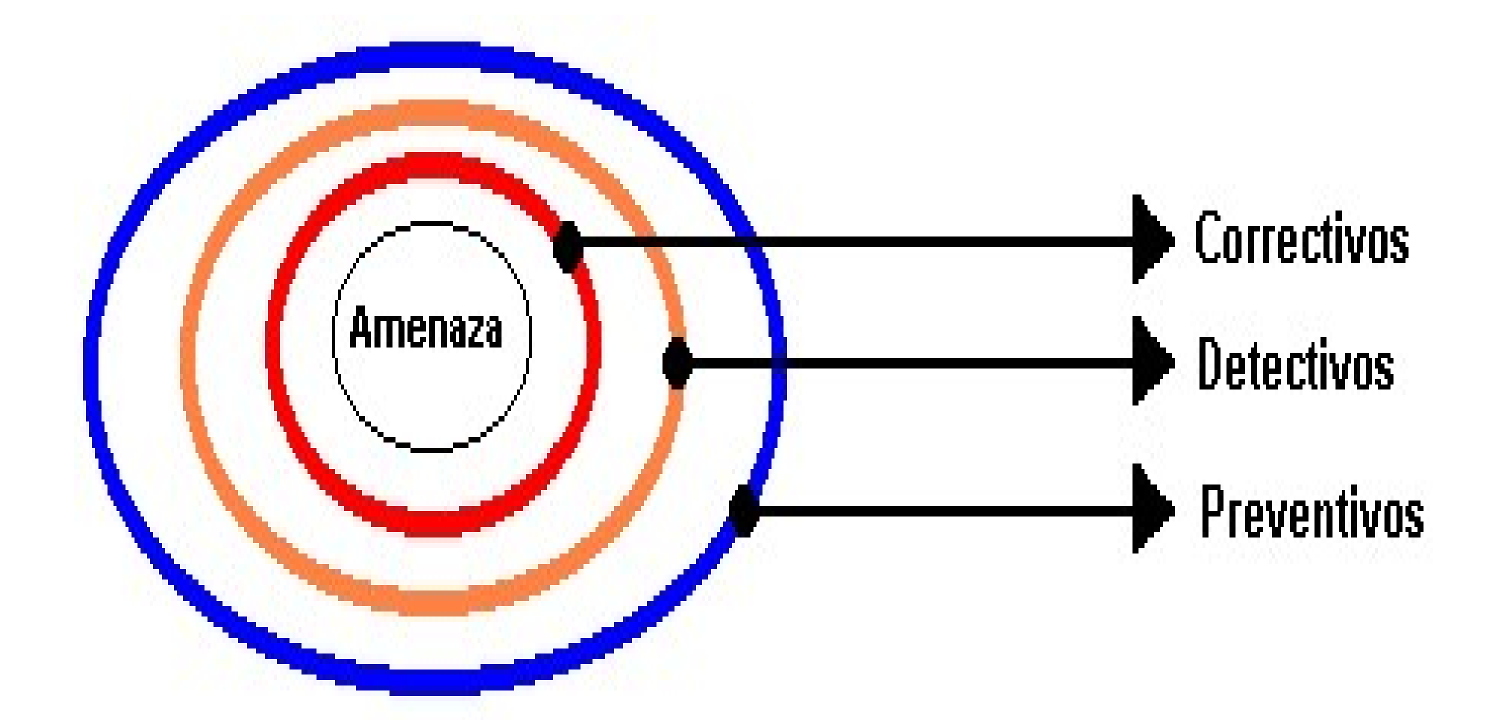
Los tres (3) Anillos de Seguridad o Líneas de Defensa.

Los controles actúan sobre los eventos de riesgo inherentes de tres maneras, interdependientes:

- ⇨ **Control Preventivo. C**ondiciona los actos de la organización para asegurar que ocurran de manera preestablecida – **Son estándares de actuación.**
- ⇨ **Control Detectivo.** Para detectar, registrar e informar la ocurrencia de la amenaza (son alarmas que se disparan cuando se detecta que está presentándose la amenaza). **Refuerzan y validan el control preventivo. Hacen pareja con el control preventivo.**
- ⇨ **Control Correctivo**. Obligan a tomar acción correctiva para resolver el problema detectado por los controles detectivos. **Hacen pareja con los controles detectivos.**



El enfoque de los 3 Anillos de Seguridad ó Líneas de Defensa







Auditoría Basada en Riesgos Críticos

Criterios para Evaluar la Efectividad de los Controles Establecidos

Niveles de Efectividad de los Controles	Criterios de Evaluación / Significado de la Efectividad de los Controles Establecidos por cada Evento de Riesgo Inherente (Amenaza)
5: Apropiada	Los controles establecidos son efectivos (eficaces y eficientes) para reducir los riesgos potenciales a nivel aceptable o tolerable de riesgo residual. Satisfacen los 3 anillos de seguridad y el nivel de automatización es aceptable o el costo beneficio es razonable. El Riesgo Residual es BAJO
4: Mejorable	Los controles satisfacen los 3 anillos de seguridad (preventivo, detectivo y correctivo), pero no son eficientes o tienen bajo nivel de automatización. Riesgo Residual es MODERADO
3: Insuficiente	Los controles utilizados no satisfacen los tres anillos de seguridad. Se necesitan controles adicionales. Riesgo Residual es ALTO.
2: Deficiente	Los controles utilizados no satisfacen los tres anillos de seguridad y no son eficientes o tienen bajo nivel de automatización. Se necesitan controles adicionales. Riesgo Residual es MUY ALTO
1: Muy Deficiente	No existen controles o los que se utilizan no sirven para controlar los riesgos potenciales. El Riesgo Residual es MUY ALTO





Aplicación del enfoque de los (3) Anillos de Seguridad o Líneas de Defensa - Ejemplo.

Evento (Amenaza): Robar dinero en cajero automático (ATM), por suplantación del propietario de la tarjeta.

Riesgo Potencial (Inherente): Evento de riesgo al que se expone el Banco (usuario), de acuerdo con la naturaleza y modo de operación del cajero automático . En su evaluación no se tienen en cuenta los controles establecidos.

Evaluación Severidad, antes de Controles : E - Extremo.

Acciones de Respuesta: Reducir (mitigar) el riesgo.

Controles:

- **Preventivos**: Uso de tarjeta y PIN. Políticas de seguridad para uso de cajero automático.
- **Detectivos:** Validar que tarjeta y PIN coincidan. Informar desviación (mensaje) y bloquear.
- **Correctivos:** Reemplazar la tarjeta bloqueada y asignar nuevo PIN.

Efectividad de los Controles. 5: Apropiada.

Riesgo Residual: Riesgo que permanece después de Evaluación de Controles y Pruebas de Auditoría. Riesgo no protegido o no cubierto por los controles establecidos. **Evaluación Severidad: B - Bajo** (Tolerable).

AUDIRISK

Informe con los Resultados de la Auditoría -

Evaluación de Efectividad de los Controles Existentes / Establecidos

Evaluación Efectividad de los Controles por Actividades del Proceso (Escenarios de riesgo).

Amenazas	Riesgo Inherente	Efectividad Controles Establecidos - Etapa 5	Riesgo Residual	Hallazgos de Auditoría
Omitir Investigación Antecedentes del cliente	E: Extremo	5: Apropiada	B: Bajo / Tolerable	
Girar Cheques con una sola firma	A: Alto	4: Mejorable	M: Moderado	1
Omitir cifras de cuadre diario	E: Extremo	3: Insuficiente	A: Alto	2,3
Alterar cifras registradas en la base de datos de cuentas corrientes	A: Alto	2: Deficiente	A: Alto	4,5
Alterar registros de Soporte de Ingresos	M: Moderado	1: Muy deficiente	M: Moderado	6
Falsificar firmas en los cheques	M: Moderado	4: Mejorable	B: Bajo / Tolerable	
Falsificar comprobantes de depósito	M: Moderado	3: Insuficiente	M: Moderado	7
Falsificar Cheques	A: Alto	1: Apropiada	B: Bajo / Tolerable	
Promedio en el Escenario	A: Alto	**3: Insuficiente**	**2: Moderado**	





Auditoría Basada en Riesgos Críticos

Medición de Riesgos Residuales, después de evaluar y verificar los Controles Establecidos - MODELO "AUDISIS“

Riesgo Inherente					
4: Extremo	Bajo	Moderado.	Alto.	Extremo	Extremo
3: Alto	Bajo	Moderado.	Alto.	Alto.	Alto.
2: Moderado	Bajo	Moderado.	Moderado.	Moderado.	Moderado.
1: Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
	5: Apropiada	4: Mejorable	3: Insuficiente	2: Deficiente	1: Muy Deficiente

Efectividad de los Controles (Protección Existente)





Evaluación Efectividad / Protección de los Controles, por Amenaza

Protección existente (PE) - Método AUDISIS	Satisfacción de los Criterios de Evaluación Efectividad	RI - Antes de Controles	RR - Después de Controles
5: PROPIADA	Se satisfacen los 3 anillos de control y por lo menos uno de los otros dos criterios (C/B = Razonable y/o Calificación promedio de los controles superior a 3.5 puntos)	4: Extremo	1: Tolerable
		3: Alto	1: Tolerable
		2: Moderado	1: Tolerable
		1: Bajo (Tolerable)	1: Tolerable
4: MEJORABLE	Se satisfacen los 3 anillos de control, únicamente	4: Extremo	2: Moderado
		3: Alto	2: Moderado
		2: Moderado	2: Moderado
		1: Bajo (Tolerable)	1: Bajo
3: INSUFICIENTE	Únicamente se satisfacen los dos criterios diferentes de los 3 anillos (C/B = Razonable y/o Calificación promedio de los controles superior a 3.5 puntos)	4: Extremo	3: Alto
		3: Alto	3: Alto
		2: Moderado	2: Moderado
		1: Bajo (Tolerable)	1: Tolerable
2: DEFICIENTE	Se satisface únicamente uno de los dos criterios diferentes de los 3 anillos (C/B = Razonable y/o Calificación promedio de los controles superior a 3.5 puntos)	4: Extremo	4: Extremo
		3: Alto	3: Alto
		2: Moderado	2: Moderado
		1: Bajo (Tolerable)	1: Bajo (Tolerable)
1: MUY DEFICIENTE	No existen controles	4: Extremo	4: Extremo
		3: Alto	3: Alto
		2: Moderado	2: Moderado
		1: Bajo (Tolerable)	1: Bajo (Tolerable)





Diseño Pruebas de Auditoría Según Resultados de la Evaluación de Control Interno

BC DE AUDITORÍA

Muestra de Eventos de Riesgo Inherente Seleccionados para Auditoría

1

Seleccionar Evento de Riesgo Inherente

Efectividad Controles =“5 Apropiada”

SI

Diseñar y Ejecutar Pruebas de Cumplimiento (PC)

NO

Efectividad Controles = “4 Mejorable”

SI

NO

Resultados Satisfactorios

SI

1

NO

2

2

Generar Hallazgos de Auditoría PC

Diseñar y Ejecutar Pruebas Sustantivas (PS)

Resultados Satisfactorios

NO

Generar Hallazgo de Auditoría PS

SI

Ultimo Evento

SI

Generar Reportes e Informes de Auditoría

Finalizar

NO

1





Selección de Riesgos (Amenazas) para Pruebas de Auditoría

Selección de Amenazas para Pruebas de Auditoría, según resultados de la Evaluación del Control Interno.

Eventos de Riesgo Inherentes (Amenazas)	Riesgo Inherente	Efectividad Controles Establecidos - Etapa 5	Pruebas de Cumplimiento Etapa 6	Controles a verificar	Pruebas Sustantivas - Etapa 7	Datos a Verificar
Omitir Investigación Antecedentes del cliente	E: Extremo	5: Apropiada	Si	1,3,10, 12		
Girar Cheques con una sola firma	A: Alto	4: Mejorable	Si	3,5,8		
Omitir cifras de cuadre diario	E: Extremo	3: Insuficiente			Si	Vr Efectivo recibido; Vr Efectivo pagado
Alterar cifras registradas en la base de datos de cuentas corrientes	A: Alto	2: Deficiente			Si	Saldo disponible; vr cheques pagados
Alterar registros de Soporte de Ingresos	M: Moderado	1: Muy deficiente			Si	Vr depósitos recibidos;
Falsificar firmas en los cheques	M: Moderado	4: Mejorable	Si	1,2,3,5		
Falsificar comprobantes de depósito	M: Moderado	3: Insuficiente			Si	Saldo disponible
Falsificar Cheques	A: Alto	5: Apropiada	Si	4,7,9		





Pruebas de Cumplimiento y Sustantivas

Estructura de Checklists de Pruebas de Cumplimiento y Sustantivas.

- Se Generan por Sitios de Prueba, técnicas de auditoría y amenazas.
- El software genera Checklist con cuatro Opciones de Respuesta que tienen puntajes asociados:
  - **5**: Siempre (Satisfactorio).
  - **4**: Casi Siempre (Con excepciones no significativas).
  - **3**: Algunas Veces (con excepciones significativas.
  - **0**: Nunca (No satisfactorio).
- Espacios para: Ref a PT, Fecha ejecución y Comentarios del auditor.





Pruebas de Cumplimiento

Evaluación de Resultados de las Pruebas, por Amenaza

Amenaza: Alteración de los datos de los datos registrados en documentos fuente.

No	CONTROLES ESTABLECIDOS	5: Siempre	4: Casi Siempre	3: Algunas Veces	0: Nunca	Tecnica de Verificacion	REF A PT	Hallazgos de Auditoria
1	Control 1	x						
2	Control 2		x					
3	Control 3		x					
4	Control 4		x					
5	Control 5	x						
6	Control 6	x						
7	Control 7				x			
	% Cumplimiento	77.14%						
	Riesgo Residual	22.86%						





Pruebas de Cumplimiento

Etapa 6: Logística para su Ejecución.

- Estas pruebas se realizan por SITIO DE PRUEBA.
- Una dependencia (área organizacional o tercero) puede tener varios Sitios de Prueba.
- Por cada amenaza se mide el porcentaje (%) de cumplimiento de los controles establecidos y el Riesgo Residual (RR).
- Por cada amenaza que tenga porcentaje de cumplimiento de los controles inferior al 80%, se generan hallazgos de auditoría.
- Por cada Sitio de Prueba se produce informe con los resultados de la Verificación del **Cumplimiento de los Controles establecidos** (Informes ejecutivo y detallado)**.**
- Los informes de los sitios de prueba se consolidan por Dependencias.





Resultados de las Pruebas de Cumplimiento de los Controles y Riesgo Residual (*)

Ejemplo.

COMPARACION DE PROTECCION EXISTENTE (PE) ANTES Y DESPUES DE PRUEBAS DE LOS CONTROLES

Amenazas	Riesgo I. Antes de Controles-Etapa 2	PE Según Eval de Controles-Etapa 5	% Puntaje Obtenido en Pruebas de Cumplimiento-Etapa 6	Cumplimiento Según Pruebas Etapa 6	PE Después de Pruebas-Etapa 6	RR Después de Pruebas-Etapa 6 (*)
Amenaza 1	4: Extremo	5: Apropiada	83%	Satisfactorio	5: Apropiada	1: Tolerable
Amenaza 2	3: Alto	5: Apropiada	70%	No Satisfactorio	4: Mejorable	2: Moderado
Amenaza 3	4: Extremo	4: Mejorable	65%	No Satisfactorio	3: Insuficiente	3: Alto
Amenaza 4	3: Alto	5: Apropiada	48%	No Satisfactorio	2: Deficiente	3: Alto
Amenaza 5	3: Alto	5: Apropiada	18%	No Satisfactorio	1: Muy Deficiente	3: Alto

(*) La Severidad del riesgo residual nunca puede ser mayor que el riesgo inherente





Resultados de las Pruebas de Auditoría - De Cumplimiento y Sustantivas

Criterios para Evaluar los resultados de las Pruebas de Auditoría.

Rangos	% de Puntaje Obtenido (PO)	Protección Existente (PE) Según *Cumplimiento / Exactitud de la Información*	Riesgo Residual – RR- (después de Pruebas) (*)
1	Mayor del 80 %	5: Apropiada	1: Aceptable
2	Entre 60 y 80%	4: Mejorable	2: Moderado
3	Entre 40 y 60%	3: Insuficiente	3: Alto
4	Entre 20 y 40%	2: Deficiente	4: Extremo
5	Menor del 20%	1: Muy deficiente	5: Extremo

(*) La Severidad del Riesgo Residual no podrá ser mayor que la Severidad Riesgo Inherente





Pruebas Sustantivas

Etapa 7: Logística para su Ejecución.

- **Objetivo:** Verificar (obtener evidencia) la exactitud de la información que maneja el proceso, que pudiera ser impactada por amenazas con las debilidades o deficiencias de control en etapas 5 y 6.
- **Diseño centralizado.** Se diseñan y planean por técnica de auditoría, para datos que pudieran ser impactados por amenazas con debilidades de control interno (protección NO APROPIADA en etapa 5) o que en etapa 6 (pruebas de cumplimiento) se comprueba que no cumplen satisfactoriamente los controles establecidos.
- **Ejecución Descentralizada.** El plan de pruebas se aplica en múltiples Sitios de Prueba de las dependencias (Áreas organizacionales o terceros) seleccionados a criterio del auditor.





Aplicar Pruebas Sustantivas

Productos a Obtener. Resumen Evaluación de la Exactitud de la Información (EI) y el Riesgo Residual (RR) por **Áreas Organizacionales / Sitios de Prueba.**

Areas / Sitios de	Puntaje Obtenido	EI Despues de Pruebas Sustantivas	Riesgo Residual despues de Pruebas	Hallazgos de Auditoria
Sitio 1	83.6 %	5: Satisfactorio	1: Bajo (Tolerable)	
Sitio2	74%	4: Mejorable	2: Moderado	1
Sitio 3	32%	2: Deficiente	4: Extremo	2,3
Sitio 4	61%	3: Insuficiente	3: Alto	4
Promedio	**41,75%**	**3: Insuficiente**	**3: Alto**	





Auditorías Basadas en Riesgos Críticos

Fase III: Comunicación de Resultados de la Auditoría.

Comprende las actividades de Generación, validación y emisión de tres (3) Informes:

- **De la Evaluación de Control Interno Existente – Etapa 5**. Para las 3 dimensiones del Cubo de Riesgos.
- **De las Pruebas de cumplimiento – Etapa 6.**
  - Por sitios de prueba.
  - Consolidado del proceso a nivel organización.
- **De las Pruebas Sustantivas – Etapa 7.**
  - Por sitios de prueba.
  - Por Áreas Organizacionales – varios sitios de prueba.
  - Consolidado del proceso a nivel organización.
  - Para las 7 características de la información de negocios.





Módulo 5:
Seguimiento a Hallazgos de Auditoria y Planes de Mejoramiento



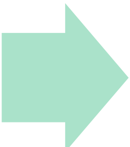


El Software AUDIRISK

Qué es y para que sirve?

MODULO 5:

Seguimiento a Hallazgos de Auditoría y Acciones de Mejoramiento.



- El software provee acceso a los auditados, por cada auditoría, para ingresar planes de acción por hallazgo y avances de implantación.
- Generación y envío automático de Correos Electrónicos de Recordatorio, a responsables de implantar, supervisar y hacer seguimiento a acciones de mejora.
- Genera estadísticas del estado de implantación de las acciones de mejora (implantadas, en proceso, pendientes de atender, anulados).





Módulo 5:

Seguimiento a Hallazgos de Auditoria y Planes de Mejoramiento

Perfil Auditores:

- Actúan como Supervisores del Seguimiento e Implantación de Acciones de Mejora.
- Asignan responsables de implantar plan de mejoramiento para atender los Hallazgos de Auditoría.
- Crea a los responsables como usuarios con perfil Auditado.
- Aprueban el Plan de Mejoramiento.
- Aceptan o No aceptan los Avances de Implantación de las Acciones de Mejora.
- Envía correos de notificación de asignación de responsables de implantar Acciones de Mejora.
- Se realiza por Sitios de Prueba, en diferentes fechas de corte.





Módulo 5:

Seguimiento a Hallazgos de Auditoria y Planes de Mejoramiento

Perfil Auditores

- Generación y envío automático de **Correos Electrónicos de Recordatorio**, a responsables de implantar, supervisar y hacer seguimiento a acciones de mejora.

- Genera estadísticas del estado de implantación de acciones de mejora (implantadas, en proceso, pendientes de atender, anulados). Por Auditoría y todas las auditorías.





Módulo 5:

Seguimiento a Hallazgos de Auditoria y Planes de Mejoramiento

Perfil Auditados:

- Actúan como Implantadores de las Acciones de Mejora requeridas para atender los hallazgos de auditoría.
- Proponen Plan de Mejoramiento a consideración de los Auditados.
- Ingresan Acciones de Mejora para atender los hallazgos de auditoría y recomendaciones de la auditoria.
- Ingresan Avances de Implantación de Acciones de Mejora.
- Corrigen y reingresan los avances de implantación no aceptados por el perfil auditor.
- Envía correos de notificación de ingreso del plan de mejoramiento y de ingreso de avances de implantación
- Se realiza por Sitios de Prueba, en diferentes fechas de corte.





Módulo 5:

Seguimiento a Hallazgos de Auditoria y Planes de Mejoramiento

Perfil Auditores

- Generación y envío automático de **Correos Electrónicos de Recordatorio**, al perfil Auditor, informando ingreso de Acciones de Mejora y Avances de Implantación.

- Genera estadísticas y visualizaciones del estado de implantación de acciones de mejora por Auditoría.





Módulo 5:

Seguimiento a Hallazgos de Auditoria y Planes de Mejoramiento

Perfil Auditados

- Generación y envío automático de **Correos Electrónicos de Recordatorio**, a responsables de implantar, supervisar y hacer seguimiento a acciones de mejora.

- Genera estadísticas del estado de implantación de acciones de mejora (implantadas, en proceso, pendientes de atender, anulados). Por Auditoría y todas las auditorías.





Módulo 6:

Gestión de Resultados de la Auditoría



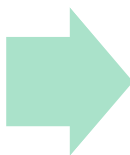


El Software AUDIRISK

Qué es y para que sirve?

MODULO 6:

Gestión de Resultados de la Auditoría.



Informes de Gestión de la Auditoría. Estadísticas y gráficos de Auditorías realizadas:

- Hallazgos de Auditoría: Control Interno (CI), pruebas de Cumplimiento (PC) y pruebas Sustantivas (PS).
- Recomendaciones Emitidas: CI; PC; PS.
- Estado de las Recomendaciones.
- Auditorías Programadas y Ejecutadas.
- Horas Cargables por Auditoría y Auditor.
- Costos por Auditoría y Auditor.





Módulo 6:

Gestión de Resultados de la Auditoría

Genera estadísticas y gráficos sobre las auditorías realizadas con AUDIRISK durante un periodo de tiempo.

- ✓ Auditorías Planeadas Vs Auditorias Ejecutadas.

- ✓ Estadísticas de Hallazgos informados en el periodo, por auditorías y tipos de Auditorías (Procesos del Modelo de Operación, Procesos de TI, Aplicaciones de Computador).

    - Cantidad y Porcentaje de Hallazgos de Auditoría sobre Diseño de Controles Internos.
    - Cantidad y Porcentajes de Hallazgos de Auditoría sobre Pruebas de Cumplimiento.
    - Cantidad y Porcentajes de Hallazgos de Auditoría sobre Pruebas Sustantivas.





Módulo 6:
Gestión de Resultados de la Auditoría

Genera estadísticas y gráficos sobre las auditorías realizadas con AUDIRISK durante un periodo de tiempo.

- ✓ Auditorías Planeadas Vs Auditorias Ejecutadas.
- ✓ Estadísticas de Hallazgos informados en el periodo, por auditorías y tipos de Auditorías (Procesos del Modelo de Operación, Procesos de TI, Aplicaciones de Computador).
  - Cantidad y Porcentaje de Hallazgos de Auditoría sobre Diseño de Controles Internos.
  - Cantidad y Porcentajes de Hallazgos de Auditoría sobre Pruebas de Cumplimiento.
  - Cantidad y Porcentajes de Hallazgos de Auditoría sobre Pruebas Sustantivas.





Módulo 6

Gestión de Resultados de la Auditoría

Genera estadísticas y gráficos sobre las auditorías desarrolladas con AUDIRISK durante un periodo de tiempo.

✓ Estadísticas sobre el **Estado de Atención** de las recomendaciones emitidas en el periodo, por auditoría, tipos de auditorías y Sitios de Prueba.

- Recomendaciones de Auditoría sobre Efectividad (Diseño) de Controles Internos.
- Recomendaciones de Auditoría sobre Pruebas de Cumplimiento.
- Recomendaciones de Auditoría sobre Pruebas de Cumplimiento.





Módulo 6:

Gestión de Resultados de la Auditoría

Genera estadísticas y gráficos sobre las auditorías desarrolladas con AUDIRISK durante un periodo de tiempo.

✓ **Estados de Atención** de las recomendaciones emitidas por la Auditoría, en el periodo.

- Implantada.
- En Proceso.
- Pendiente (por iniciar implantación).
- Anulada.





Módulo 6:

Informes de Gestión de la Auditoría

AUDIRISK

AudiRisk Web

Software de Auditoria Basada en Riesgos

Producto Licenciado a AUDISIS LTDA

Usuarios en línea: 1

24/09/2015

Cerrar sesión Ayuda

Auditorías basadas en riesgos | Seguimiento Auditorias de Terceros | Enfoque Rapido Auditorias

Usted esta en: Inicio > AudiRisk > Gestión de la auditoria > Auditorías basadas en riesgos > Estadisticas recomendaciones auditorías ejecutadas

Nombre Empresa: Morraos de Colombia

Estadisticas recomendaciones de auditoría

Año Fiscal 2015

Fecha Inicial * ... Fecha Final * ... Filtrar Consultar Todo

Por tipo auditoría | Consolidado por tipo auditoría

Seleccione Tipo Auditoria

1 - Aplicaciones de Computador

Auditoría	Recomendaciones CI	Recomendaciones PC	Recomendaciones PS	Totales	Porcentaje (%)
2 - Software Contable	4	1	1	6	100.00
Total	4	1	1	6	100.00
Porcentaje	66.67	16.67	16.67		

Estadísticas de Recomendaciones por tipos de auditoría Reporte





Agenda

- AudiRisk: Qué es y para Qué Sirve?.
- Características del Software AudiRisk que agregan valor a las Organizaciones y las Auditorías.
- Especificaciones Generales y Técnicas del Software AudiRisk.
- Presentación Detallada de Módulos Componentes del Software AudiRisk.
- **Beneficios de Utilizar AudiRisk.**
- Usuarios del software AudiRisk.





Beneficios de Utilizar AUDIRISK?





Beneficios Corporativos

Con el Enfoque Proactivo y Preventivo de AUDIRISK:

- Se incrementa la calidad, confiabilidad y eficiencia de los servicios de auditoría.
- La auditoría ofrece mayor valor agregado a la empresa.
- Promueve el mejoramiento de la cultura de **medición** de efectividad, eficiencia y cumplimiento de los controles internos.





Beneficios para las Dependencias que manejan las Operaciones

Con el Enfoque Proactivo y Preventivo de AUDIRISK:

- Recibirán informes de auditoría más proactivos y asesores.
- Los resultados de la auditoría servirán como apoyo para promover la eficiencia y efectividad *del monitoreo de los controles* que deben realizar los propietarios de la información de negocios.





Beneficios para el Departamento de Auditoría

Con el Enfoque Proactivo y Preventivo de AUDIRISK:

Se facilita un cambio real en la imagen del departamento dentro de la organización, basado en:

- Auditorías más proactivas y preventivas que reactivas y a posteriori.
- Imagen del auditor “asesor-consultor” de la Organización.
- Incrementa productividad, eficiencia y efectividad de la auditoría.





Beneficios para el Departamento de Auditoría

Con el Enfoque Proactivo y Preventivo de AUDIRISK:

- ⇨ **Estandariza** los procedimientos y prácticas de auditoría (planeación, ejecución, informes y seguimiento) en las revisiones de los procesos de negocio o sistemas de información sujetos a auditoría.

- ⇨ **Automatiza** los procedimientos y prácticas de auditoría para evaluación de riesgos, evaluación y verificación de controles, verificación de exactitud de la información y seguimiento a recomendaciones de la auditorías.





Beneficios para el Departamento de Auditoría

Con el Enfoque Proactivo y Preventivo de AUDIRISK:

⇨ Automatiza la actualización y consulta de **bases de conocimientos** que contienen las “best practices” de administración de riesgos, control interno y auditoría utilizadas por la empresa en sus procesos de negocio y de tecnología de información.





Beneficios para el Auditor

Con el Enfoque Proactivo y Preventivo de AUDIRISK:

Motiva cambios importantes en la imagen y credibilidad de los auditores:

- ❑ Mejorar su imagen, efectividad y credibilidad dentro de la organización.
- ❑ Obtener mayor credibilidad y aceptación en la comunidad profesional.





Beneficios para el Auditor

Con el Enfoque Proactivo y Preventivo de AUDIRISK:

- Los auditores crecen profesionalmente con la transferencia tecnológica que reciben.
- Los auditores actúan más como asesores que como investigadores.





Agenda

- AudiRisk: Qué es y para Qué Sirve?.
- Características del Software AudiRisk que agregan valor a las Organizaciones y las Auditorías.
- Especificaciones Técnicas del Software AudiRisk.
- Requerimientos de Hardware y Software para instalar AUDIRISK.
- Productos que recibe el Usuario de AUDIRISK.
- Beneficios de Utilizar AudiRisk.
- **Usuarios del software AudiRisk.**





Usuarios de AUDIRISK en Colombia y el Exterior

En Colombia.

Sector Industrial.

- Petróleos del Norte . PETRONORTE.
- Caracol TV.
- Oleoducto Central de Colombia- OCENSA.
- Lafayette S.A.
- Monómeros Colombo Venezolanos.





Usuarios de AUDIRISK en Colombia y el Exterior

En Colombia.

Sector Financiero.

- Global Securities – Medellín.
- Crediservir – Cooperativa de Ahorro y Crédito – Ocaña.
- Valor Alta – Comisionista de Bolsa.
- Crezcamos – Ahorro y Crédito. Bucaramanga.
- Financiera Andina - Finandina S. A.
- Fundación Mundial de la Mujer – Bucaramanga.
- FINAGRO.

Sector Salud.

- Salud Vida – EPS – Auditoría Interna.
- Famisanar – EPS – Auditoría Interna.





Usuarios de AUDIRISK en Colombia y el Exterior

En Colombia.

Cajas de Compensación Familiar.

- Comfenalco Tolima.
- Caja de Compensación Comfamiliares Caldas.
- Caja de Compensación Familiar de Arauca - COMFIAR.
- Compensar.





Usuarios de AUDIRISK en Colombia y el Exterior

En Colombia.

Entidades del Sector Público.

- Policía Nacional
- Empresa Electrificadora de Santander - ESSA.
- Contraloría General de la República
- Armada Nacional.
- Instituto Nacional de Vías – INVIAS.
- Instituto Agustín Codazzi.
- Secretaría de Hacienda – Bogotá.





Usuarios de AUDIRISK en Colombia y el Exterior

En Colombia.

Sector Educativo

- Universidad Militar Nueva Granada.
- Universidad Pedagógica y Tecnologíca de Colombia.
- Universidad La Gran Colombia – Bogotá.
- Universidad de Ibagué – Coruniversitaria.
- Universidad Autónoma de Cali.
- Universidad Jorge Tadeo Lozano.
- Universidad EAFIT.
- Universidad Santo Tomás de Bucaramanga.
- Universidad Católica de Colombia.





Usuarios de AUDIRISK en Colombia y el Exterior

Firmas de Auditores.

- MGI Páez y Asociados Auditores y Consultores.
- Nexia Montes y Asociados.
- Colombian Consulting Group.
- Datos y Procesos (Pasto).





Usuarios de AUDIRISK en Colombia y el Exterior (cont.)

En el Exterior.

- Cooperativa Sagrada Familia- Tegucigalpa – Honduras.
- Universidad Peruana Unión (UPEU).
- Banco Central de la República Dominicana.
- Banco Central del Ecuador.
- Banco Centroamericano de Integración Económica (BCIE) - Honduras.
- Banco Santacruz – Bolivia.
- Cervecería de Costa Rica.
- Instituto Nacional de Seguros (Costa Rica).





Usuarios de AUDIRISK en Colombia y el Exterior (cont.)

En el Exterior.

- Auditoría General de Bancos (Costa Rica).
- Banco Nacional de Costa Rica.
- Cía. Nal. de Fuerza y Luz (Costa Rica).







Gracias por su Atención

Hasta Pronto !

Para conocer el software ingrese a www.softwareaudisis.com

